HP CloudSystem 8.0 Administrator Guide

Abstract

This information is for use by administrators using **HP CloudSystem Foundation and Enterprise Software 8.0**, who are assigned to configure and provision compute resources for deployment and use in virtual data centers. This guide provides instructions on using the CloudSystem Foundation Console and Portal user interfaces, as well as introducing the CloudSystem command line interface. Built on OpenStack technology, CloudSystem supports most OpenStack Havana functionality available in Nova, Keystone, Neutron, Cinder, Glance, and Horizon components. This guide describes limitations on this OpenStack functionality in this software release. Additionally, this guide provides information necessary to configure the full use of CloudSystem Enterprise.

HP Part Number: 5900-3376
Published: March 2014
Edition: 1

Microsoft® and Windows® are U.S. registered trademarks of the Microsoft group of companies.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

The open source code used by HP CloudSystem is available on the HP web at http://www.hp.com/software/opensource.

Contents

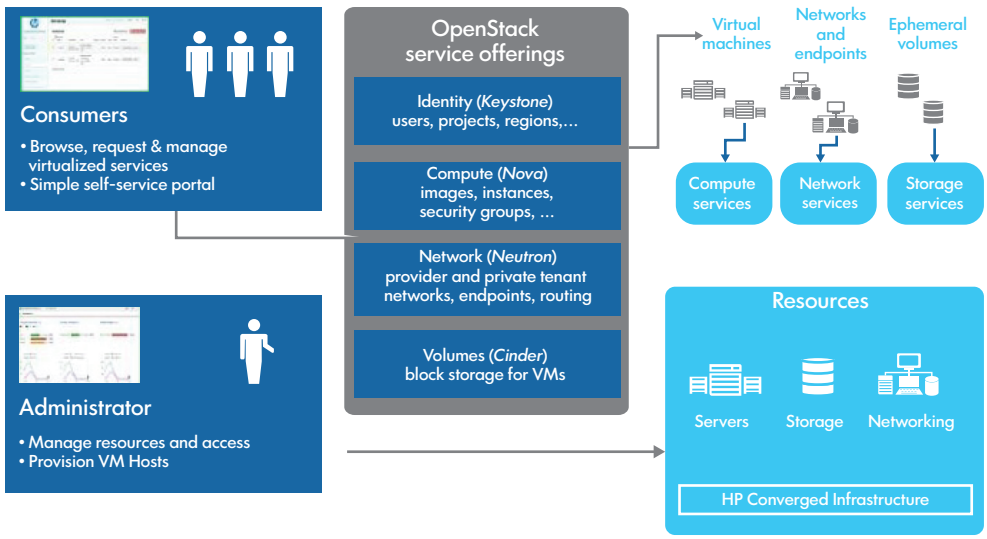
Part I Understanding HP CloudSystem

1 Welcome to HP CloudSystem Administrator Guide

HP CloudSystem works in converged infrastructure environments and provides a software-defined approach to managing the cloud. CloudSystem consists of two offerings:

- **HP CloudSystem Foundation** is based on the HP Cloud OS distribution of OpenStack Cloud Software. It integrates hardware and software to deliver core Infrastructure as a Service (IaaS) provisioning and lifecycle management of compute, network and storage resources. You can manage CloudSystem Foundation from an administrative console, self-service portal, CLIs, and OpenStack APIs. It provides an appliance-based deployment console to simplify installation and maintenance, and an embedded version of HP Operations Orchestration (OO) for automating administrative processes. See CloudSystem Foundation components (page 18) for more information.

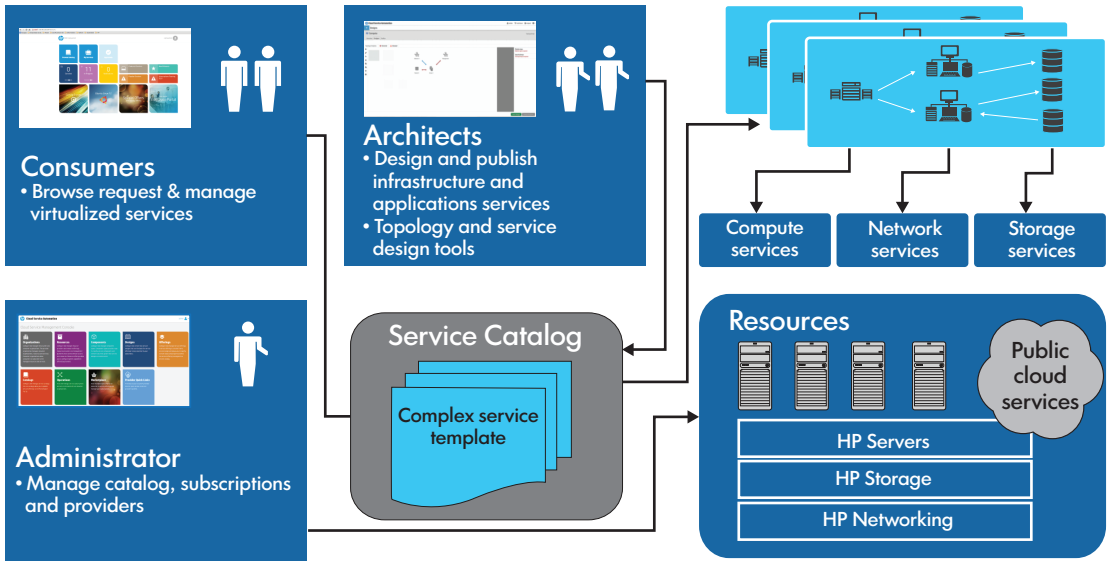
Figure 1 CloudSystem Foundation



- **HP CloudSystem Enterprise** expands on CloudSystem Foundation to integrate servers, storage, networking, security, and management to automate the lifecycle for hybrid service delivery. Template architects can use Enterprise to create infrastructure templates and offer them as services in a Marketplace Portal. Users select services from a catalog and manage their subscriptions. When a service is requested, Enterprise automatically provisions the servers,

storage, and networking. Enterprise also includes an enhanced set of Operations Orchestration workflows. See CloudSystem Enterprise components (page 20) for more information.

Figure 2 CloudSystem Enterprise



Features

Features in CloudSystem allow you to:

- **Easily install and upgrade** CloudSystem, which is a set of virtual machine appliances connected by multiple networks.

  See CloudSystem Foundation components (page 18) and Monitor resource use and allocation in CloudSystem Console (page 112).

- **Manage the lifecycle of your infrastructure**, including monitoring its health, using an administrator user interface that simplifies adding and managing cloud services.

  See Monitor resource use and allocation in CloudSystem Console (page 112) and About the Console Dashboard (page 112).

- **Create and activate compute nodes**, which have software installed and configured that enables the compute node to be added to the cloud.

  See Compute node creation (page 96) and Compute node management (page 103).

- **Configure provider networks**, which allow you to connect pre-existing physical networks to the cloud, and private networks, which allow groups of users to share private resources exclusively inside their virtual data center or cloud.

  See Network configuration (page 73).

- **Configure virtual server storage** to connect 3PAR storage systems to compute nodes.

  See Storage configuration (page 89).

- **Create, upload, and manage operating system images.** A created image is a snapshot of an active instance. You can also track which images are in use and on which virtual machines.

  See Image management (page 84).

- **Define and configure virtual machines**. The number of CPUs and amount of memory to assign to a virtual machine is designated by selecting the flavor (instance type) to associate with a virtual machine.

  See Virtual machine configuration for compute services (page 108).
- **Deploy virtual machine instances** with VLAN networks and HP 3PAR virtual machine block storage using the CloudSystem Portal.

  See Provision a cloud in Foundation (page 117).
- **Use HP Operations Orchestration workflows** to automate operational tasks and processes. See CloudSystem Foundation components (page 18).
- **Install CloudSystem Enterprise**. CloudSystem Foundation uses OpenStack technology to provision and manage cloud services. CloudSystem Enterprise uses CloudSystem Foundation for appliance management and provides added value through the user interface, capacity planning/analytics, high availability, disaster recovery, and more.

  See About CloudSystem Enterprise (page 124).
- **For high availability, use the features of VMware vCenter Server** when the cloud is deployed on ESX clusters. For KVM, a CloudSystem white paper describes setting up an HA environment on the management cluster in which CloudSystem runs.
- **Use OpenStack API technology** for portability and developer community access.
- **Issue OpenStack commands** for supported operations using a Windows or Linux client.

2 Concepts and architecture

CloudSystem provides you with the flexibility of virtualized compute resources, networks, and storage. With CloudSystem, you configure, manage, and deploy infrastructure services into a cloud environment for access by your end users.

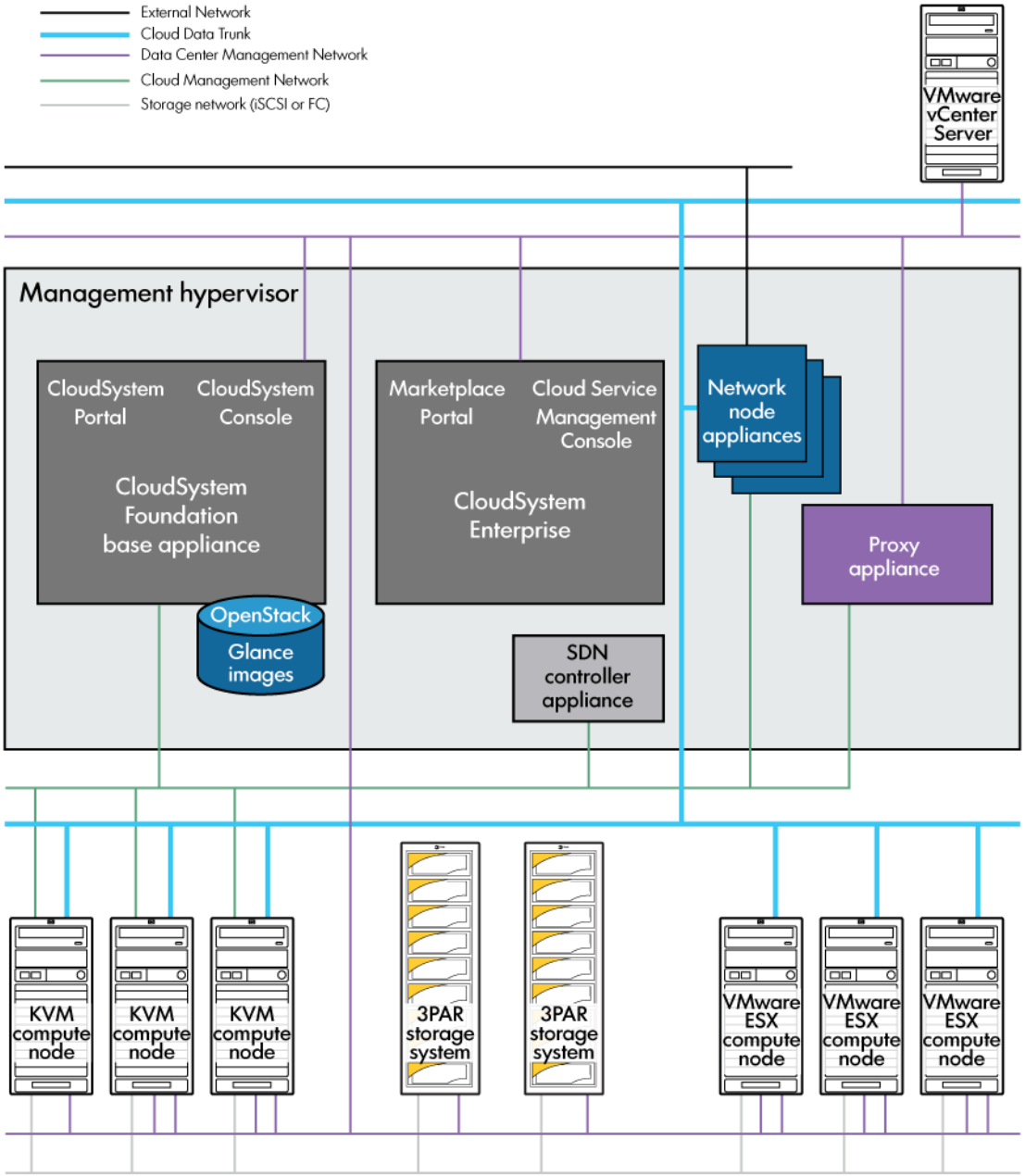
How it works

Figure 3 illustrates the relationship between CloudSystem Foundation, the Foundation virtual appliances, CloudSystem Enterprise, and the underlying network infrastructure.

The CloudSystem Foundation base appliance includes a management console GUI and a web-based, end-user portal that is built on OpenStack Horizon functionality. The base appliance includes the data store for Glance images that can be used to build the compute virtual machines. The installation of CloudSystem Foundation also includes the SDN appliance, the network node appliances, and a vCenter Server proxy appliance.

From within the CloudSystem Console, you can install the Enterprise piece of CloudSystem. Enterprise provides significant manageability and design tool extensions and cloud-bursting to multiple providers through the HP CSA Cloud Service Management Console. Access to these services is provided to end users through the Marketplace Portal. Once you install the Enterprise software, you can move between Foundation and Enterprise user interfaces to manage, provision, and deploy cloud services.

Figure 3 CloudSystem appliances and network infrastructure



See the *HP CloudSystem Installation and Configuration Guide* at the Enterprise Information Library for an expanded discussion of network architecture and initial network configuration.

Associated appliances

The following appliances are automatically created after the Cloud Networking settings are saved.

For more information, see Networks in CloudSystem Foundation (page 19).

Software Defined Networking (SDN) appliance Manages the network infrastructure for the CloudSystem.

Network node appliances Manage network services, such as DHCP and L3 (routing) services, for provisioned virtual machines and provisioned virtual networks. Three network node appliances are created when the Cloud Networking settings are saved.

The following appliance is automatically created after an ESX cluster is imported. (No proxy appliances are started in a KVM-only environment.)

Proxy appliance — Acts as a communication mechanism between OpenStack technology and VMware vCenter Server, and runs the OpenStack agents for up to twelve clusters for each vCenter Server. Additional appliances are automatically created when the number of new clusters added to the cloud are reached. New proxy appliances are created with the first, 13th, and 25th cluster additions.

Storage

CloudSystem works with **HP 3PAR StoreServ Storage**, a cluster-based storage architecture that incorporates data management and fault tolerance technologies that can meet the storage needs of smaller sites and can be scaled for global organizations.

3PAR storage is required to create block storage for VM guests.

Storage for manually provisioned hypervisor hosts is more flexible, and can include local disks.

Virtual server storage

Virtual server storage connects the 3PAR storage system to virtual machine instances. Options include:

- Fibre Channel Storage Area Network (**FC SAN**), which provides block-level storage that can be accessed by the applications running on any networked servers
- **Direct-Attach Fibre Channel Storage**, a single-layer Fibre Channel storage network that eliminates SAN switches and HBAs (host bus adapters)
- **iSCSI**, which is block-level storage that uses traditional Ethernet network components for connectivity

Physical servers

Servers running an ESX cluster or a KVM hypervisor can be used as a management cluster, a management hypervisor, or as compute clusters or nodes.

Management cluster or hypervisor — Clustered or standalone hypervisors that host the virtual machine appliances that comprise the CloudSystem solution. There are three possible configurations:

- An ESX management cluster that hosts the virtual machines running CloudSystem and its integrated tools.
- A standalone ESX management hypervisor that hosts the virtual machines running CloudSystem and its integrated tools.

  See also Integrated tool connectivity and configuration (page 81).
- A KVM management hypervisor that hosts the virtual machines running CloudSystem software.

Compute nodes — ESX clusters and KVM hosts that provide the pool of hypervisor resources used to provision virtual machine instances.

User authentication

You can choose one of two methods of user authentication. If you use local logins, CloudSystem provides local authentication for users authorized to access CloudSystem. The Infrastructure administrator enters user data, which is saved in the appliance database. When anyone tries to

access the CloudSystem Console or Portal, the login information entered is checked against the user attributes stored in the database.

Alternatively, you can use an external authentication directory service (also called an enterprise directory) to provide a single sign-on for groups of users instead of maintaining individual local login accounts. Examples of an authentication directory service include Microsoft Windows Active Directory or OpenLDAP (LDAP - Lightweight Directory Access Protocol).

For more information, see Security in CloudSystem (page 22) and Manage users and groups (page 52).

OpenStack technology

CloudSystem software leverages the capabilities of multiple OpenStack technologies. Because of this underlying functionality, you can use OpenStack CLI and API to configure compute resources, and provision and deploy these resources to a cloud.

Table 1 OpenStack clients used in CloudSystem

Client	Service	Capability
Cinder	Block storage management	Create, configure, and assign storage volumes and volume types
Glance	Image management	Create, configure and store images
Keystone	Identity management	Create users and manage user roles and credentials
Neutron	Network management	Configure Private (and External) networks
Nova	Compute resource management	Manage virtual machine instances, flavors, and images and deploy instances to a cloud

For additional information on installing and using the OpenStack CLI with CloudSystem software, see the "Command line interfaces" appendix in the *HP CloudSystem 8.0 Installation and Configuration Guide* at Enterprise Information Library.

The CloudSystem Portal is based on the Openstack Horizon client. Not all OpenStack features are supported in this version of CloudSystem. For information on limitations, see Limitations on support for OpenStack CLI commands (page 204) and Limitations on support for OpenStack functionality in the CloudSystem Portal (page 210).

CloudSystem Foundation at a glance

HP CloudSystem allows you to prepare private cloud resources and deploy virtual machine instances into this cloud. In CloudSystem Foundation, you use CloudSystem Console to configure cloud resources for deployment. This includes creating images, establishing shared and private networks, and configuring block storage. End users use the CloudSystem Portal to provision and manage VMs, storage, and networks. This work includes managing virtual machine security, attaching volumes, and launching virtual machine instances.

When you provision new subscriptions from CloudSystem Enterprise, new virtual machines, block storage volumes, and networks are provisioned in CloudSystem Foundation. These resources are visible in the CloudSystem Portal. If you modify them from the CloudSystem Portal, the changes will not be reflected in the Enterprise Marketplace Portal.

CloudSystem Foundation components

CloudSystem Foundation is the platform that you use to manage both Foundation and Enterprise appliances. Foundation includes the following components, which run on virtual machine appliances on the management cluster or hypervisor.

CloudSystem Console — Web-based user interface for administrative tasks, including managing and monitoring the cloud and releasing resources

	back to the cloud. From the console, you can activate compute nodes, configure networks and storage, and perform maintenance tasks on the Foundation and Enterprise appliances.
CloudSystem Portal	Web-based interface for creating, launching, and managing virtual machine instances. The portal can be accessed by appending **/portal** to the Foundation appliance URL (for example, `https://192.0.2.2/portal`).
HP Operations Orchestration	Operations Orchestration Central automates operational tasks and processes using a set of predefined workflows. OO Central is packaged with the Foundation appliance and is launched from the Integrated Tools screen in the CloudSystem Console. Enterprise integrates with OO Central to support pre- and post-server group provisioning. Operations Orchestration Studio is an optional tool for customizing workflows, which is installed separately. The OO Studio installation files are included with the CloudSystem installation tar files. See the *HP CloudSystem Installation and Configuration Guide* on the Enterprise Information Library for more information.
Command line interface	**csadmin** provides command line access for storage system administrative tasks, private network VLAN management tasks, appliance management tasks and console user management tasks. **csstart** deploys and configures the Foundation base appliance on the management cluster or hypervisor. For a more friendly user experience, launch the csstart GUI; or you can run csstart from the command line.

Networks in CloudSystem Foundation

CloudSystem Foundation is built on OpenStack Networking technology. The underlying network infrastructure is managed by a Software Defined Networking (SDN) appliance. Multiple network node appliances manage network services, such as DHCP and routing. A vCenter proxy appliance runs the OpenStack agents for use. All of these virtual appliances to support networking are automatically created when CloudSystem Foundation is configured. You can use the CLI to access and manage these appliances.

CloudSystem Foundation uses three types of networks:

- **Private networks** are restricted and can be accessed only by virtual machine instances assigned to the network. See About Private Networks (page 76).
- **Provider networksisc.prov.ntwks.name;** are shared networks in the data center on which users can provision any number of virtual machine instances. See About Provider Networks (page 74).
- The **External Network** allows you to route virtual machine instances on Private networks out from the CloudSystem private cloud to the data center, the corporate intranet, or the Internet.. See About the External Network (page 77).

See also How it works (page 15).

Network tasks and user roles

The following table lists CloudSystem network tasks according to user roles and the interfaces used to perform them.

Task	User Role	Interface	Additional information
Create pools of VLAN IDs and VLAN ranges that can be assigned to Private Networks	Infrastructure administrator	CloudSystem Console	About Private Networks (page 76)
Create Provider networks	Infrastructure administrator	CloudSystem Console	About Provider Networks (page 74)
Complete the External Network configuration	Infrastructure administrator	CloudSystem Portal	About the External Network (page 77)
Customize network offerings using supported APIs	Infrastructure administrator	Foundation base appliance command line	*OpenStack Networking API v2.0 Reference*
Attach Private networks to instances	Cloud user	CloudSystem Portal	*OpenStack End User Guide*
Create routers to connect networks	Cloud user	CloudSystem Portal	*OpenStack End User Guide* and Creating an External Network router (page 79)
Manage IP addresses using either dedicated static IPs or DHCP	Cloud administrator	CloudSystem Portal	*OpenStack End User Guide*
Access instances that are on Private networks from outside of the cloud using floating IP addresses	Cloud user	CloudSystem Portal	*OpenStack End User Guide* and Assigning floating IP addresses to instances (page 79)

CloudSystem Enterprise at a glance

To install CloudSystem Enterprise, select the **Enterprise** screen on the main menu in the CloudSystem Console and click **Install CloudSystem Enterprise**. After installation, the Enterprise screen in the CloudSystem Console provides links to HP Cloud Service Automation and the Marketplace Portal. You will continue to use the Foundation platform to perform appliance management tasks after Enterprise is installed.

CloudSystem Enterprise components

Enterprise includes the following components:

HP CSA Cloud Service Management Console

HP Cloud Service Automation orchestrates the deployment of compute and infrastructure resources and complex multi-tier application architectures. HP CSA and its user interface, the Cloud Service Management Console, integrates and leverages the strengths of several HP data center management and automation products, adding resource management, service offering design, and a customer portal to create a comprehensive service automation solution.

Marketplace Portal

The Marketplace Portal provides a customer interface for requesting new cloud services and for monitoring and managing existing services, with subscription pricing to meet your business requirements.

Topology Designer and **Sequential Designer**

The HP CSA graphical service design and content portability tools simplify developing, leveraging, and sharing an array of service offerings that can be tailored to your end users' needs.

You can use two different designers to design new cloud services with reusable service design templates.

- Use Topology Designer to create infrastructure service designs.
- Use Sequential Designer to create more complex application service designs.

  The designs created through both designers appear as service offerings that Marketplace Portal users can select and provision.

3 Security in CloudSystem

CloudSystem security depends in part on the security level that you chose when you installed CloudSystem Foundation and on your work practices. This chapter describes security concepts to consider when working with browsers, certificates, and networks for secure communication and transfer of data among the appliances, networks, and computes nodes in a CloudSystem virtualized data center.

For additional information, see Manage security (page 67) and the *HP CloudSystem Installation and Configuration Guide* on the Enterprise Information Library.

Best practices for maintaining a secure appliance

Most security policies and practices used in a traditional environment apply in a virtualized environment. However, in a virtualized environment, these policies might require modifications and additions.

The following table comprises a partial list of security best practices that HP recommends in both physical and virtual environments. Differing security policies and implementation practices make it difficult to provide a complete and definitive list.

Topic	Best Practice
Accounts	• Limit the number of local accounts. Integrate the appliance with an enterprise directory solution such as Microsoft Active Directory or OpenLDAP.
Certificates	• Use certificates signed by a trusted certificate authority (CA), if possible. CloudSystem uses certificates to authenticate and establish trust relationships. One of the most common uses of certificates is when a connection from a web browser to a web server is established. The machine level authentication is carried out as part of the HTTPS protocol, using SSL. Certificates can also be used to authenticate devices when setting up a communication channel. The appliance supports self-signed certificates and certificates issued by a CA. The appliance is initially configured with self-signed certificates for the web server, database, and message broker software. The browser will display a warning when browsing to the appliance using self-signed certificates. HP advises customers to examine their security needs (that is, to perform a risk assessment) and consider the use of certificates signed by a trusted CA. For the highest level of security, HP recommends that you use certificates signed by a trusted certificate authority: ◦ Ideally, you should use your company's existing CA and import their trusted certificates. The trusted root CA certificate should be deployed to user's browsers that will contact systems and devices that will need to perform certificate validation ◦ If your company does not have its own certificate authority, then consider using an external CA. There are numerous third-party companies that provide trusted certificates. You will need to work with the external CA to have certificates generated for specific devices and systems and then import these trusted certificates into the components that use them. As the Infrastructure administrator, you can generate a CSR (certificate signing request) and, upon receipt, upload the certificate to the appliance web server. This ensures the integrity and authenticity of your HTTPS connection to the appliance. Certificates can also be uploaded for the database and message broker.
Network	• Do not connect management systems (for example, the appliance, the iLO card, and Onboard Administrator) directly to the Internet. If you require access to the Internet, use a corporate VPN (virtual private network) that provides firewall protection.
Nonessential services	• The appliance is preconfigured so that nonessential services are removed or disabled in its management environment. Ensure that you continue to minimize services when you configure host systems, management systems, network devices (including network ports not in use) to significantly reduce the number of ways your environment could be attacked.
Passwords	• For local accounts on the appliance, change the passwords periodically according to your password policies. • Password contains between 8 and 40 characters • The following special characters are not allowed: `< > ; , " ' & / \ | + =`
Roles	• Clearly define and use administrative roles and responsibilities; for example, the Infrastructure administrator performs most administrative tasks.
Service Management	• Consider using the practices and procedures, such as those defined by the *Information Technology Infrastructure Library* (ITIL). For more information, see the following website: http://www.itil-officialsite.com/home/home.aspx

Topic	Best Practice
Updates	• Ensure that a process is in place to determine if software and firmware updates are available, and to install updates for all components in your environment on a regular basis.
Virtual Environment	• Most security policies and practices used in a traditional environment apply in a virtualized environment. However, in a virtualized environment, these policies might require modifications and additions. • Educate administrators about changes to their roles and responsibilities in a virtual environment. • Restrict access to the appliance console to authorized users. For more information, see Restricting console access (page 24). • If you use an Intrusion Detection System (IDS) solution in your environment, ensure that the solution has visibility into network traffic in the virtual switch. • Maintain a zone of trust, for example, a DMZ (demilitarized zone) that is separate from production machines. • Ensure proper access controls on Fibre Channel devices. • Use LUN masking on both storage and compute hosts. • Ensure that LUNs are defined in the host configuration, instead of being discovered. • Use hard zoning (which restricts communication across a fabric) based on port WWNs (Worldwide Names), if possible. • Ensure that communication with the WWNs is enforced at the switch-port level.

Enabling or disabling authorized services access

When you first start up the appliance, you can choose to enable or disable access by on-site authorized support representatives. By default, on-site authorized support representatives are allowed to access your system through the appliance console and diagnose issues that you have reported.

Support access is a root-level shell, which enables the on-site authorized support representative to debug any problems on the appliance and obtain a one-time password using a challenge/response mechanism similar to the one for a password reset.

Any time after the initial configuration of the appliance, you can enable or disable services access through the UI by selecting **Actions→Edit services access** on the **Settings** window.

You can also use an `appliance/settings` REST API to enable or disable services access.

NOTE: HP recommends that you enable access. Otherwise, the authorized support representative might be unable to access the appliance to correct a problem.

Restricting console access

For the virtual appliance, you can restrict console access through secure management practices of the hypervisor itself.

For VMware vSphere, this information is available from the VMware website:

http://www.vmware.com

In particular, search for topics related to vSphere's Console Interaction privilege and best practices for managing VMware's roles and permissions.

Best practices for browser use

- Enable SSL v3 and TLS.

  SSL v2 is considered insecure and should not be enabled in the browser unless there is a specific need for it.

- Enable cookies to store the authenticated user's session ID.

- Always log out before closing the browser.

  In the browser, a memory-based cookie stores the authenticated user's session ID. Memory-based cookies are deleted when you close the browser. When you log out, the session on the appliance is invalidated.

- Avoid clicking links outside the appliance UI.

  While logged in to the appliance, avoid clicking links in email or instant messages. The links might be malicious and take advantage of your login session.

- Use separate browsers for appliance and non-appliance use.

  Do not use the same browser instance (for example, separate tabs in the same browser) to browse to other websites.

Managing certificates from a browser

A certificate authenticates the appliance over SSL. The certificate contains a public key, and the appliance maintains the corresponding private key, which is uniquely tied to the public key.

NOTE: This section discusses certificate management from the perspective of the browser. For information on how a non-browser client (such as cURL) uses the certificate, see the documentation for that client.

The certificate also contains the name of the appliance, which the SSL client uses to identify the appliance.

The certificate has the following boxes:

- **Common Name (CN)**

  This name is required. By default it contains the fully qualified host name of the appliance.

- **Alternative Name**

  The name is optional, but HP recommends supplying it because it supports multiple names (including IP addresses) to minimize name-mismatch warnings from the browser.

  By default, this name is populated with the fully qualified host name (if DNS is in use), a short host name, and the appliance IP address.

  NOTE: If you enter **Alternative Name**s, one of them must be your entry for the **Common Name**.

Self-signed certificate

The default certificate generated by the appliance is self-signed; it is not issued by a trusted certificate authority.

By default, browsers do not trust self-signed certificates because they lack prior knowledge of them. The browser displays a warning dialog box; you can use it to examine the content of the self-signed certificate before accepting it.

Protecting credentials

Local user account passwords are stored using a salted hash; that is, they are combined with a random string, and then the combined value is stored as a hash. A hash is a one-way algorithm that maps a string to a unique value so that the original string cannot be retrieved from the hash.

Passwords are masked in the browser. When transmitted between appliance and the browser over the network, passwords are protected by SSL.

Local user account passwords must be a minimum of eight characters, with at least one uppercase character. The appliance does not enforce additional password complexity rules. Password strength

and expiration are dictated by the site security policy. If you integrate an external authentication directory service (also known as an enterprise directory) with the appliance, the directory service enforces password strength and expiration.

4 Installation

A successful install and configuration of CloudSystem software depends on the preparation done beforehand. See the *HP CloudSystem Installation and Configuration Guide* on the Enterprise Information Library for the following information.

- Supported hardware and software configurations
- Preparations necessary prior to installing CloudSystem
- Network configuration details
- HP Operations Orchestration configuration
- Installing CloudSystem Enterprise
- Troubleshooting installation
- `csstart` command reference
- Configuring additional virtualization providers to work with CloudSystem Enterprise

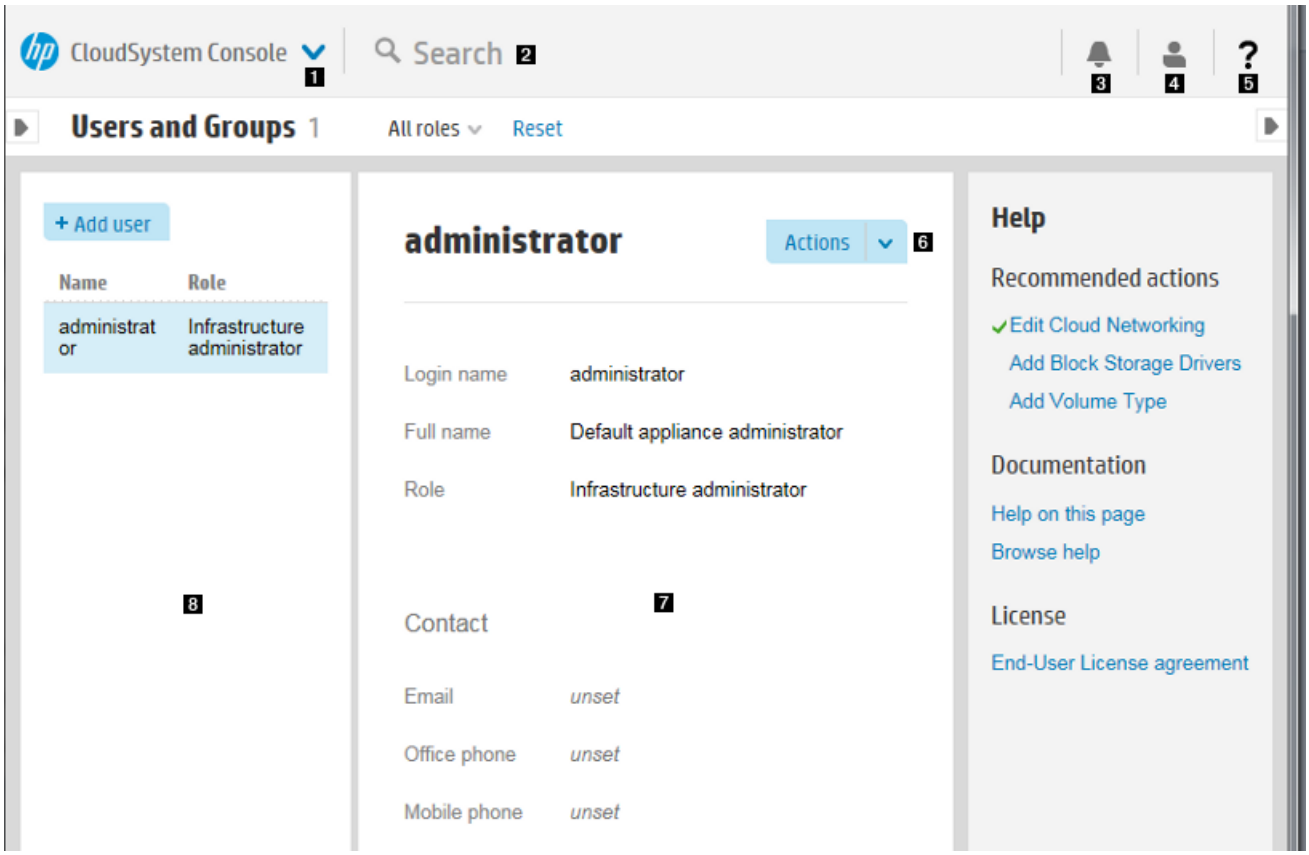
5 Navigating the CloudSystem Console GUI

This chapter provides you with an overview of the GUI functions in the CloudSystem Console. More information about using these features is located in the CloudSystem Console Help.

About the graphical user interface

The image shown below illustrates important areas in the CloudSystem Console graphical user interface.

Figure 4 Screen components



1. **Main menu**: Access the primary resource management areas of the appliance for compute, networking, and storage resources, and for appliance administration. (To see the main menu, click in the gray area labeled CloudSystem Console.)
2. **Search**: Enter a search term. The **Scope** option allows you to restrict your search to the resource you are on, or widen the search to all resources managed by the CloudSystem Console. (To see the Scope selector, click on or near the word "Search".)
3. **Activity sidebar**: View alerts and notifications generated by the appliance.

   Click the Activity icon , then click the left or right pin icons to expand or collapse this sidebar.
4. **Session control**: View the status of your login, or log out of the appliance.
5. **Help sidebar**: View links to online help and to recommended actions. **Recommended actions** include tasks needed to configure the appliance or to prepare resources for provisioning to a cloud.

   Click the Help icon , then click the left or right pin icons to expand or collapse this sidebar.

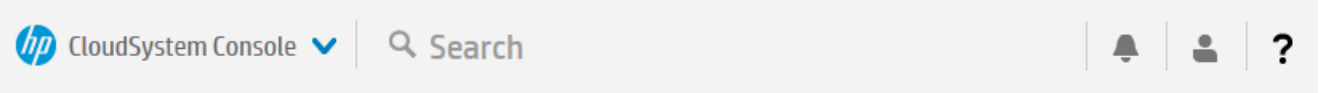
6 **Actions menu**: Access the available actions that you can perform on a resource. **Actions** menus contain only tasks that can be performed on a specific resource.
7 **Details pane**: View the details for the resource area you have open.
8 **Master pane**: Manage the display of information in the Details pane for each specific resource. You can use filters and sorting to control the display of information.

Use the banner and main menu to navigate

Use the **main menu** to navigate through the resources and actions that the appliance provides.

To expand the main menu, click the ⌄ in the banner at the top of the screen.

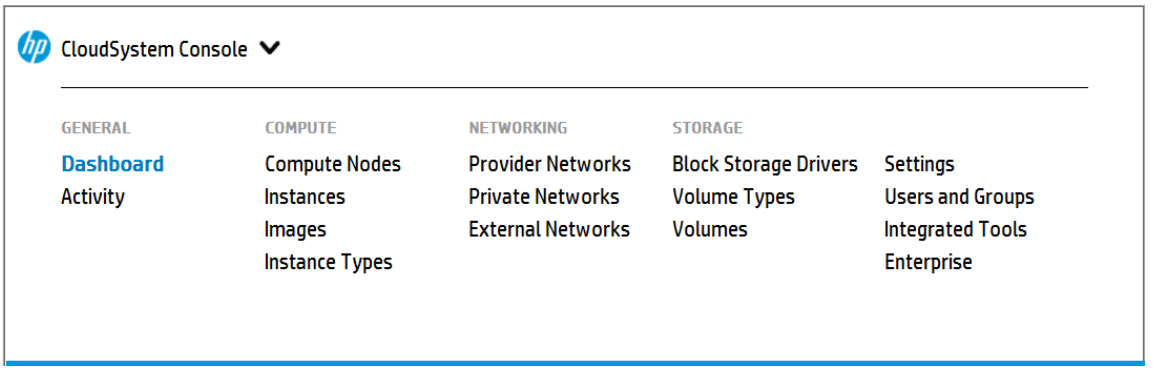
Figure 5 Main menu and top of page banner



The main menu provides access to resources and actions. The following figure shows the expanded menu.

NOTE: Your ability to view a resource or perform an action depends on your role.

Figure 6 Main menu

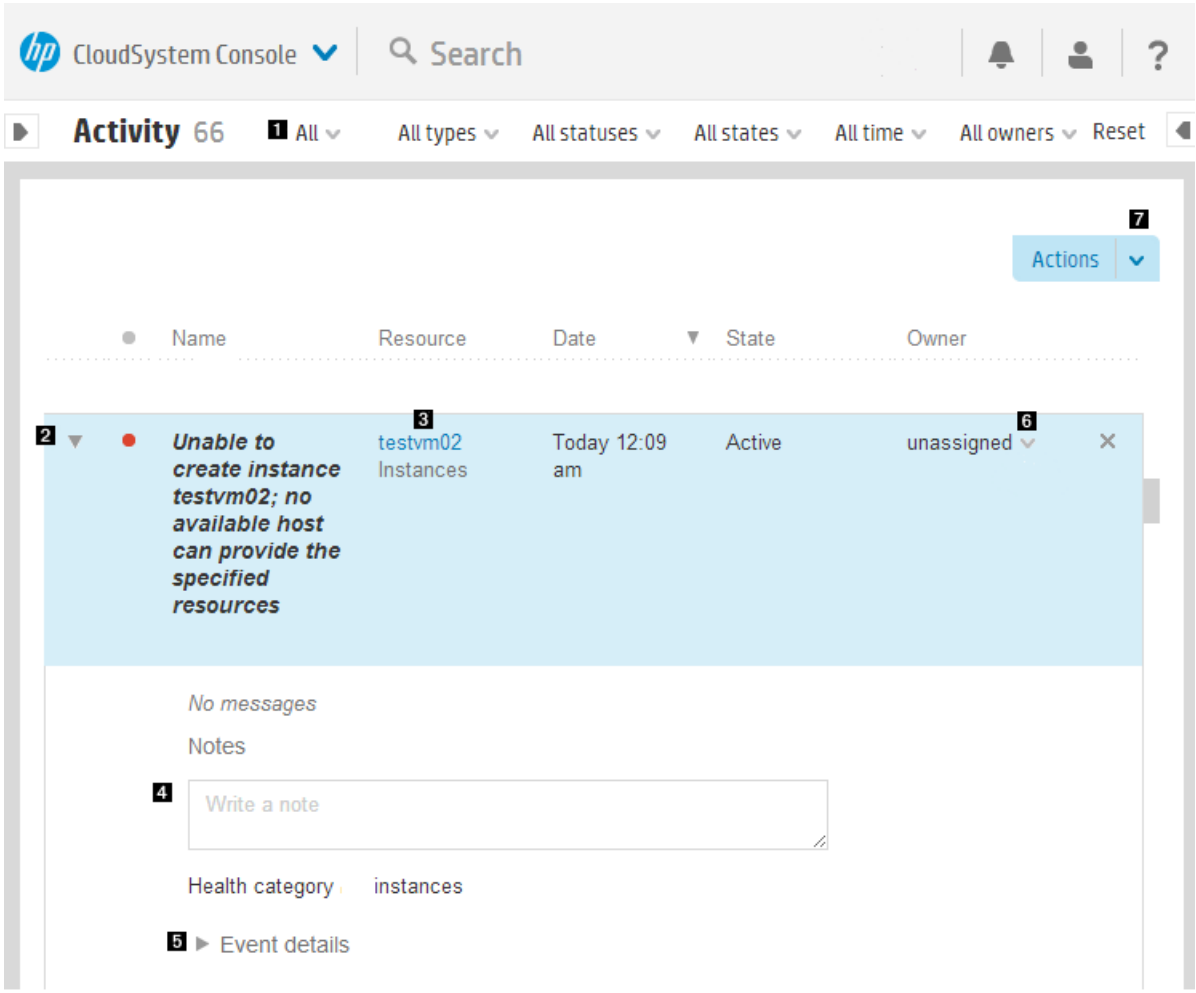


About Activity

The **Activity** overview screen lists alerts and other notifications about activities occurring in your cloud environment. You can filter, sort, and expand areas of the screen to refine how information is displayed. Links within activity details enable you to view additional information about specific resources listed.

Activity Screen components

You can use the screen areas shown below to monitor and interpret **Activity** data.



1. The default **Activity** view shows all active notifications. Use the filters and date range selectors on the **Filters** menu bar to filter all stored notifications.

   You can also click the icon to expand (or collapse) the filter banner, which contains the same selection choices in a vertical presentation.
2. Click the ▸ icon to expand the view of a notification, or click the ▾ icon to collapse the view.
3. Click the link to view details about the resource associated with this notification. If multiple events have sent the same notification, a count is given.
4. Type in the note box to add instructions or other information to this notification.

TIP: You can click and drag the lower right corner of the note box to expand the box for better viewing or easier editing.

---

5. Click the ▸ icon to view more details about this notification.
6. Click the ▾ icon and select from the list to assign (or reassign) an **Owner** for this notification.
7. Use the **Actions** menu to assign, clear, or restore selected notifications.

About alerts

The appliance uses alert messages to report issues with the resources it manages. The resources generate alerts to notify you that some meaningful event occurred and that an action might be required.

An event is a single, low-level problem or change that occurred on a resource. Usually, events are detected by an agent running either on the resource or on the appliance.

Each alert includes the following information about the event it reports: severity, state, description, and urgency. You can clear alerts, assign owners to alerts, and add notes to alerts.

While alerts have an active or locked state, they contribute to a resource's overall displayed status. After you change their state to `Cleared`, they no longer affect the displayed status.

IMPORTANT:
The appliance keeps a running count of incoming alerts. At intervals of 500 alert messages, the appliance determines if the number of alerts has reached 75,000. When it does, an auto-cleanup occurs, which deletes alert messages until the total number is fewer than 74,200. When the auto-cleanup runs, it first removes the oldest cleared alerts. Then it deletes the oldest alerts by severity.

About tasks

All user-initiated tasks are reported as activities. User-initiated tasks are created when a user adds, creates, removes, updates, or deletes resources.

The **Activity** screen provides a valuable source of monitoring and troubleshooting information that you can use to resolve an issue. You can determine the type of task performed, whether the task was completed, when the task was completed, and who initiated the task.

IMPORTANT: The appliance maintains a task database that holds information for approximately six months or 50,000 tasks. If the task database exceeds 50,000 tasks within the six-month period, the oldest blocks of 500 tasks are deleted until the count is fewer than 50,000. Tasks older than six months are removed from the database.

The task database and the database that stores alerts are separate.

About the Activity sidebar

The **Activity** sidebar shows tasks initiated during the current session. The most recent task is displayed first.

Task notifications provide information (including in-progress, error, and completion messages) about tasks that were launched.

The **Activity sidebar** differs from the **Activity** screen because it displays only recent activity. The **Activity** screen, in contrast, displays all activities and allows you to list, sort, and filter them. For more information, see About Activity (page 29).

Click an activity to show more details.

Activity states

Activity	State	Description
Alert	**Active**	The alert has not been cleared or resolved. A resource's active alerts are considered in the resource's overall health status. Active alerts contribute to the alert count summary.
	Locked	An `Active` alert that was set (locked) by an internal resource manager. You cannot manually clear a `Locked` alert. Examine the corrective action associated with an alert to determine how to fix the problem. After the problem is fixed, the resource manager moves the alert to the `Active` state. At that time, you can clear the alert. A resource's locked alerts contribute to its overall status.
	Cleared	The alert was addressed, noted, or resolved. You clear an activity when it no longer needs to be tracked. The appliance clears certain activities automatically.

Activity	State	Description
		`Cleared` activities do not affect the resource's health status and they are not counted in the displayed summaries.
Task	**Completed**	The task started and ran to completion.
	Running	The task has started and is running, but has not yet completed.
	Pending	The task has not yet run.
	Interrupted	The task ran, but was interrupted. For example, it could be waiting for a resource
	Error	A task failed or generated a `Critical` alert. Investigate `Error` states immediately.
	Terminated	A task was gracefully shut down or cancelled.
	Warning	An event occurred that might require your attention. A warning can mean that something is not correct within the appliance. Investigate `Warning` states immediately.

Activity statuses

Status	Description
Critical	A critical alert message was received, or a task failed or was interrupted. Investigate `Critical` status activities immediately.
Warning	An event occurred that might require your attention. A warning can mean that something is not correct within the appliance and it needs your attention. Investigate `Warning` status activities immediately.
OK	For an alert, `OK` indicates normal behavior or information from a resource. For a task, `OK` indicates that it completed successfully.
Unknown	The status of the alert or task is unknown. The status of a task that is set to run at a later time is `Unknown`.
Disabled	A task was prevented from continuing or completing.

Icon descriptions

HP CloudSystem uses icons as user controls and to show the current status of resources and activities.

Status and severity icons

Large icon	Small icon	Resource	Activity Notification	Explanation
		Error	Critical	Failed/Interrupted. Investigate immediately. See also Troubleshooting reference (page 138).
		Warning	Warning	Component is active but issues exist that can impact performance. Investigate and determine what action to take.

Large icon	Small icon	Resource	Activity Notification	Explanation
		OK	Informational	Component is active. No action needed.
		Unknown	Informational	Component is not known to the cloud and is not in an active state within the cloud. Determine if intervention is needed.
		An **In progress** rotating icon indicates that a change is being applied or a task is running. This icon can appear in combination with any of the resource states; for example: 		

User control icons

Icon	Name	Action
	Expand menu	Expands a menu to show all options
	View details	Identifies a title that has additional information. Clicking the title changes the view to display details.
	Expand	Expands a collapsed list item
	Collapse	Collapses an expanded list item
	Edit	Enables editing
	Delete or remove	Deletes the current entry
	Search	Searches for the text you enter in the **Search** box. This is especially useful for finding types of resources or specific resources by name
	Pin	The left pin collapses or expands the **Filters** pane. The right pin docks the **Activity** and **Help** sidebars.
	Sort	Determines whether items are displayed in ascending or descending order

Informational icons

Icon	Name	Description
	Activity control	Provides information about recent task activities for operations, user actions, and resources
	Session control	Displays your login name and the duration of your current session. Also provides a link you can use to log out of the appliance.
	Help control	• When this icon is at the top of a dialog box, you can click it to open context-sensitive help for that topic in another window or tab. • In the banner, this icon expands or collapses the **Help** sidebar, where you can browse the help documentation or find help on the screen currently displayed. The help sidebar provides the following: ◦ A **Help on this page** hyperlink to access context-sensitive help for the current screen ◦ A **Browse help** hyperlink to access the entire help system ◦ Links that you can use to display the EULA and the Written Offer.

Browser requirements

The appliance has specific browser requirements that can affect its use. The following browsers are supported:

- Microsoft Internet Explorer: Version 9 and Version 10
- Mozilla Firefox: ESR Version 24, Personal edition (latest version)
- Google Chrome Version 31

Required browser plug-ins and settings

The following browser settings must be enabled for the software to work correctly:

- JavaScript
- Image loading
- SSL 3.0 or TLS 1.0 security options
- Session cookies
- Adobe Flash plugin version 10 or later

Supported browser features and settings

Screen resolution — For optimum performance, the screen size should be at least 1280×1024 pixels for desktop monitors, or 1280×800 for laptop displays. The minimum supported screen size is 1024×768 pixels.

Close window — Browser windows can be closed at any time. Closing the window while you are logged in automatically ends your session so that another user cannot connect to it.

NOTE: Closing the browser tab does not end your session.

Copy and paste — Almost any text can be selected and copied. However, text that is part of an image cannot be selected and copied. You can paste into text entry fields.

Language	This version is available in US English, Japanese, and Simplified Chinese. Set your browser language preference to one of these languages. To ensure that server-generated messages are displayed in the same language as the browser displays, set the **Locale** in the **Time and Language** section of the **Settings: Appliance** screen to match the browser language.

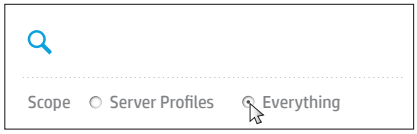
Search resources

The banner of every screen includes the **Smart Search** feature, which enables you to find resource-specific information such as specific instances of resource names, serial numbers, WWNs (World Wide Names), and IP and MAC addresses.

In general, anything that appears in a resource master pane is searchable.

Smart Search makes locating resources easy, enabling you to inventory or take action on a desired set of resources.

The default search behavior is to focus on the resource you are currently viewing. But, to broaden the scope of your search across all resources, you have the option to search **Everything**, which searches all resources.

Search the current resource	Search all resources
1. Click in the **Smart Search** box. 	**1.** Click in the **Smart Search** box. 
2. Enter your search text and press **Enter**. The search results are focused in your current location in the UI.	**2.** Select **Everything**.  **3.** Enter your search text and press **Enter**.

Some resources might not include the option to choose between the current resource or everything, in which case the default search is for everything.

When you start typing, search suggestions are provided based on pattern matching and previously-entered search criteria.

- You can either select a suggestion (the screen displays data containing that selection) or click **Enter**.
- If your search term is a resource, then the list of resources in a master pane is filtered to match your search input.

TIP:

- Enter complete words or names as your search criteria. Partial words or names might not return the expected results.
- If you enter a multi-word search term, results show matches for all words you enter.
- Enclose a search term in double quotes (") if the search term contains spaces.

When you find what you are looking for in the search results, which are organized by type, select the item to navigate to it.

Table 2 Advanced searching and filtering with properties

Example of advanced filtering syntax	Search results

By model name:
`model: "BladeSystem c7000 Enclosure G2"`
`model: "ProLiant BL460c Gen8"`
`model: "HP VC 8Gb 20-Port FC Module"`
	All hardware that match the model number and name.

By name or address: `name: enclosure10`	An enclosure with the name `enclosure10`.
`name: "192.0.2"`	A list of virtual machines whose IP addresses begin with `192.0.2`.
`name: "mysystem"`	A list of virtual machines for which the host name is `mysystem`.
By health status: `status: Critical`	All resources that are in a critical state. For other health status values, see Activity statuses (page 32).

6 Support and other resources

IMPORTANT: This product contains a technical feature that will allow an on-site authorized support representative to access your system, through the system console, to assess problems that you have reported. This access will be controlled by a password generated by HP that will only be provided to the authorized support representative. You can disable access at any time while the system is running.

HP technical support personnel are not granted remote access to the appliance.

Information to collect before contacting HP

Be sure to have the following information available before you contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

Understanding the audit log

The audit log contains a record of actions performed on the appliance, which you can use for individual accountability.

You must have Infrastructure administrator privileges to download the audit log.

To download the audit log from the UI, select **Settings→Actions→Download audit log**. You must have Infrastructure administrator privileges.

Monitor the audit logs because they are rolled over periodically to prevent them from getting too large. Download the audit logs periodically to maintain a long-term audit history.

Each user has a unique logging ID per session, enabling you to follow a user's trail in the audit log. Some actions are performed by the appliance and might not have a logging ID.

A breakdown of an audit entry follows:

Token	Description
Date/time	The date and time of the event
Internal component ID	The unique identifier of an internal component
Reserved	The organization ID. Reserved for internal use
User domain	The login domain name of the user
User name/ID	The user name
Session ID	The user session ID associated with the message
Task ID	The URI of the task resource associated with the message
Client host/IP	The client (browser) IP address identifies the client machine that initiated the request

Token	Description
Result	The result of the action, which can be one of the following values: • SUCCESS • FAILURE • SOME_FAILURES • CANCELED • KILLED
Action	A description of the action, which can be one of the following values: • ADD • MODIFY • DELETE • ACCESS • RUN • LIST • ENABLE • DISABLE • SAVE • SETUP • UNSETUP • DEPLOY • START • DONE • KILLED • CANCELED • LOGIN • LOGOUT • DOWNLOAD_START
Severity	A description of the severity of the event, which can be one of the following values, listed in descending order of importance: • INFO • NOTICE • WARNING • ERROR • ALERT • CRITICAL
Resource URI/name	The resource URI/name associated with the task
Message	The output message that appears in the audit log

Example 1 Sample audit entries: user login and logout

```
2013-09-16 14:55:20.706 CST,Authentication,,,administrator,jrWI9ych,,,
SUCCESS,LOGIN,INFO,CREDENTIAL,,Authentication SUCCESS

.
.
.

2013-09-16 14:58:15.201 CST,Authentication,,,MISSING_UID,jrWI9ych,,,
SUCCESS,LOGOUT,INFO,CREDENTIAL,,TERMINATING SESSION
```

Download audit logs

The audit log shows the security administrator what security-related actions took place on the base appliance.

You can download log files and other information for your authorized support representative to use to diagnose and troubleshoot an appliance.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 1 Downloading audit logs

1. From the **Settings** screen, select **Actions→Download audit logs**.

2. The appliance generates a compressed file of the audit logs and downloads it to your local computer.

   The compressed file is named following this format:

   `audit-logs-yyyy_mm_dd-hh_mm_ss`

   yyyy_mm_dd indicates the date, and *hh_mm_ss* indicates the time the file was created. The name of the audit log file is displayed on the screen.

   The audit log file is downloaded to the default download folder. If no default download folder is configured in your browser, you are prompted to specify a destination file.

Create a support dump file

NOTE: This procedure creates a support dump for the base appliance only.

Some error messages recommend that you create a support dump of the appliance and send it to an authorized support representative for analysis. The support dump process performs the following functions:

- Deletes any existing support dump file
- Gathers logs and other information required for debugging
- Creates a compressed file with a name in the following format:

  hostname-CI-timestamp.sdmp

Unless you specify otherwise, all data in the support dump file is encrypted so that only an authorized support representative can access it.

You can choose not to encrypt the support dump file if you have an onsite, authorized support representative or if your environment prohibits outside connections. You can also validate the contents of the support dump file and verify that it does not contain sensitive data such as passwords.

The support dump file is a `gzip` of a `tar` file. Renaming your support dump to have a `.tar.gz` or `.tgz` extension can make it easier to examine the contents.

IMPORTANT: If the appliance is in an error state, you can still create an encrypted support dump file without logging in or other authentication.

The support dump file contains the following:

- Operating system logs
- Product logs
- The results of certain operating system and product-related commands

For issues regarding virtual machine instance creation and deployment, gather the following files created on the compute nodes:

- `/var/log/nova/*`
- `/var/log/isc/*`
- `/var/log/libvirt/*`
- `/etc/libvirt/*`

Items logged in the support dump file are recorded according to UTC time.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 2 Creating a support dump file

1. From the main menu, select **Settings→Actions→Create support dump**.

2. Choose whether or not to encrypt the support dump file:
   a. To encrypt the support dump file, confirm that the **Enable support dump encryption** check box is selected.
   b. To turn off encryption, clear the **Enable support dump encryption** check box.
3. Click **Yes, create**.

   You can continue doing other tasks while the support dump file is created.
4. The support dump file is downloaded when this task is completed. If your browser settings specify a default download folder, the support dump file is placed in that folder. Otherwise, you are prompted to indicate where to download the file.
5. Contact your authorized support representative for instructions on how to transfer the support dump file to HP.

   For information on contacting HP, see How to contact HP (page 41).

IMPORTANT: Unless you specify otherwise, the support dump file is encrypted so that only an authorized support representative can view its contents.

Support dump files sent to HP are deleted after use, as the HP data retention policy requires.

Enable or disable services access

With this procedure, you can allow or deny access to the base appliance by an on-site authorized support representative.

IMPORTANT: This product contains a technical feature that will allow an on-site authorized support representative to access your system, through the system console, to assess problems that you have reported. This access will be controlled by a password generated by HP that will only be provided to the authorized support representative. You can disable access at any time while the system is running.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 3 Enabling or disabling services access

1. From the **Settings** screen, select **Actions→Edit services access**.
2. Read the Warning statement on this screen carefully.
3. Select the appropriate option:
   - Select **Enabled** if you want to allow an authorized support representative to access your appliance.
   - Select **Disabled** if you want to deny an authorized support representative access to your appliance.
4. Click **OK**.

   A screen displays the setting you chose. Use the main menu to return to the **Settings** screen.

How to contact HP

Use the following methods to contact HP:

- To obtain HP contact information for any country, see the Contact HP worldwide website:
  http://www.hp.com/go/assistance
- Use the **Get help from HP** link on the HP Support Center:
  http://www.hp.com/go/hpsc
- To contact HP by telephone in the United States, use the Contact HP – Phone Assist website to determine the telephone number that precisely fits your needs. For continuous quality improvement, conversations might be recorded or monitored.
  http://www8.hp.com/us/en/contact-hp/phone-assist.html#section1

Registering for software technical support and update service

HP CloudSystem includes one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals, either in electronic form or on physical media as they are made available from HP. Customers who purchase an electronic license are eligible for electronic updates only.

With this service, HP CloudSystem customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

http://www.hp.com/services/insight

Registration for this service takes place following online redemption of the license certificate.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the U.S. HP partner and store locator website:
  http://www.hp.com/service_locator
- In other locations, see the Contact HP worldwide website:
  http://www.hp.com/go/assistance

Documentation feedback

HP is committed to providing documentation that meets your needs.

To help us improve the documentation, send your suggestions and comments to:

docsfeedback@hp.com

In your mail message, include the following information. They are located on the front cover.

- Document title
- Published date
- Edition number

Help us pinpoint your concern by posting the document title in the Subject line of your mail message.

Related information

Use this section to learn about available documentation for HP CloudSystem components and related products

HP CloudSystem documents

The latest versions of HP CloudSystem manuals and white papers can be downloaded from the *Enterprise Information Library* at http://www.hp.com/go/CloudSystem/docs, including the following documents:

- *HP CloudSystem 8.0 Release Notes*
- *HP CloudSystem 8.0 Installation and Configuration Guide*
- *HP CloudSystem 8.0 Administrator Guide*
- *HP CloudSystem Help*
- *HP CSA Concepts Guide*
- *HP CSA Release Notes*
- *HP CSA API Quick Start Guide*
- *HP CSA Troubleshooting*
- *HP CSA API Reference*
- *HP CSA Documentation List*
- *HP Operations Orchestration Concepts*
- *HP Operations Orchestration Central User Guide*
- *HP Operations Orchestration Application Program Interface (API) Guide*
- *HP CloudSystem Foundation and Enterprise Software 8.0: Recommended Backup and Restore Procedures*

Online help for the CloudSystem Console is available by clicking the help control button in the Console GUI: 

The help control button expands the help sidebar. Links in the sidebar open UI screens for **Recommended Tasks**, help for the current screen (**Help on this page**), and help for all tasks and procedures (**Browse help**).

HP Software documents

The latest versions of HP Software product manuals and white papers can be downloaded from the *HP Software Product Manuals* web site at http://support.openview.hp.com/selfsolve/manuals.

Finding documents on the HP Software Product Manuals web site

Follow these instructions to access all technical manuals for **HP Cloud Service Automation** and **HP Operations Orchestration**.

1. Go to the *HP Software Product Manuals* web site (http://support.openview.hp.com/selfsolve/manuals).
2. Log in with your HP Passport user name and password.

   OR

   If you do not have an HP Passport, click **New users — please register** to create an HP Passport, then return to this page and log in.
3. In the **Product** list box, scroll down and select a product name.
4. In the **Product Version** list, select the version of the manuals that you are interested in.
5. In the **Operating System** list, select the relevant operating system.
6. Click the **Search** button to see a list of linked titles.

HP Insight Management documents

The latest versions of HP Matrix Operating Environment manuals, white papers, and the *HP Insight Management Support Matrix* can be downloaded from the *HP Enterprise Information Library* at http://www.hp.com/go/matrixoe/docs, including the following documents:

- *HP Matrix Operating Environment Release Notes*
- *HP Insight Management Support Matrix*
- *HP Matrix Operating Environment Infrastructure Orchestration User Guide*
- *Cloud bursting with HP CloudSystem Matrix infrastructure orchestration*

Third-party documents

CloudSystem incorporates OpenStack technology (listed below), and interoperates with other third-party virtualization software.

OpenStack Havana

- *OpenStack Documentation for Havana releases*
  - *Cloud Administrator Guide*
  - *Virtual Machine Image Guide*
  - *API Quick Start*
  - *Admin User Guide*
  - *End User Guide*
    - Command reference
      - Keystone commands
      - Glance commands
      - Neutron commands
      - Nova commands
      - Cinder commands

Red Hat

- *Red Hat Enterprise Linux 6 documents*

VMware

- *VMware vSphere documents*

HP 3PAR StoreServ Storage documents

The latest versions of HP 3PAR StoreServ Storage manuals can be downloaded from the *HP Support Center*, including the following documents:

- *HP 3PAR StoreServ Storage Concepts Guide*
- *HP 3PAR StoreServ Storage Troubleshooting Guide*

Finding documents on the HP Support Center web site

Follow these instructions to access all technical manuals hosted on the HP Support Center.

1. Go to the *HP Support Center* web site (http://www.hp.com/go/support).
2. Select the **Drivers & Software** tab.
3. Type a product name in the **Find by product** box and click **Go**.

4. Select a specific product from the resulting list.
5. On the specific product support page, locate the search fields at the top right of the web page.
   The top search field will contain the product name that you selected earlier in your search.
6. In the second search field below the first, type "manuals" and press **Enter**.
   If the list of documents is long, it might take a few seconds to load the page with the search results.
7. You can refine the search results using the sorting options in the document table headers or by further refining your search criteria in the search feature that is located immediately above the document list.

HP ProLiant servers documents

- The *HP Integrated Lights-Out QuickSpecs* contain support information and are available from the iLO product website:
  http://www.hp.com/go/ilo
- HP ProLiant servers:
  - ProLiant BL BladeSystem servers:
    http://www.hp.com/go/blades
  - ProLiant DL series rack mount servers:
    http://www.hp.com/servers/dl
  - ProLiant ML series tower servers:
    http://www.hp.com/servers/ml
  - ProLiant SL series scalable system servers:
    http://h10010.www1.hp.com/wwpc/us/en/sm/WF02a/15351-15351-3896136.html

Part II CloudSystem Foundation appliances management

7 Manage the Foundation appliances

This part of the Administrator Guide will help you with tasks necessary to configuring aspects of the appliances themselves. Specifically, you can learn how to set up and manage enterprise directory users and groups, secure appliance data transfer, and manage licenses. See also Troubleshoot the CloudSystem appliances (page 141).

About managing the appliance

The Settings screen **Actions** menu contains an **Update Foundation appliances** link that allows you to download the latest software versions for the Foundation appliances. See Update Foundation appliances (page 48).

From the **Actions** menu, you can also perform support tasks such as creating audit logs, or creating a support dump file to send to HP Support for analysis. See Create a support dump file (page 39).

You can enable and disable HP support access to the base appliance. When this feature is enabled, an HP Support representative can request a one-time-use password from HP Support to log into your appliance to troubleshoot critical issues.

About Foundation appliance settings

IMPORTANT: Do not change the network configuration of the Foundation base appliance after you have installed Enterprise.

Viewing Foundation appliance settings

The Appliance pane on the **Settings** screen displays information about the CloudSystem Foundation appliance:

- Appliance resources, including LAN speed, number of vCPUs, and amount of memory
- Host name
- Network interfaces. Hover over the box to see the Foundation appliance IP address and the cloud network IP address.
- Model of the appliance
- Current date and time
- Version and date of the appliance software

To edit appliance settings, click the **Edit** icon to the right of the Appliance pane.

To view CloudSystem Enterprise appliance settings after Enterprise is installed, click **Enterprise** on the main menu.

Change the appliance host name, IP address, subnet mask, or gateway address

Prerequisites

- Minimum required privileges: Infrastructure administrator
- CloudSystem Enterprise is *not* installed

Procedure 4 Changing Appliance Networking settings

1. From the main menu, navigate to the **Settings** screen.
2. Click the **Edit** icon in the **Appliance** panel.

   If the appliance is configured with multiple network interfaces, select the specific network to edit.

3. Edit any of the appliance network characteristics. For information, click **Help on this page** in the CloudSystem Console.
4. Click **OK** to reconfigure the appliance network.

Change the DNS server

Prerequisites

- Minimum required privileges: Infrastructure administrator
- You have the IP address of the new DNS server.

Procedure 5 Changing the DNS server

1. From the main menu, navigate to the **Settings** screen.
2. Click the **Edit** icon in the **Appliance** panel.
3. Enter the IP address for the new DNS server into the **Preferred DNS server** field.

   For information on this field, click **Help on this page** in the CloudSystem Console.
4. Optionally, enter the IP address for the alternate DNS server into the **Alternate DNS server** field.
5. Ensure that **Address assignment** (for **IPv4**) is set to your preference.
6. Click **OK** to reconfigure the appliance network.

About backup and restore operations for CloudSystem Foundation

The entirety of CloudSystem Foundation cannot be backed up or restored from the Console. To learn how to back up and restore CloudSystem Foundation, see the white paper available at Enterprise Information Library.

Shut down the appliance

Use this procedure to perform a graceful shutdown of the base appliance.

Prerequisites

- Minimum required privileges: Infrastructure administrator.
- Ensure that all tasks have been completed or stopped, and that all other users are logged off.

Procedure 6 Shutting down the appliance

1. From the **Settings** screen, select **Actions→Shut down**.

   A dialog box opens to inform you that all users will be logged out and ongoing tasks will be canceled.
2. Select **Yes, shut down** in the dialog box.

Restart the appliance

Use this procedure to perform a graceful shutdown and restart of the base appliance. You are returned to the login screen.

Prerequisites

- Minimum required privileges: Infrastructure administrator.
- Ensure that all tasks have been completed or stopped, and that all other users are logged off.

Procedure 7 Restarting the appliance

1. From the **Settings** screen, select **Actions→Restart**.

   A dialog box opens to inform you that all users will be logged out and ongoing tasks will be canceled.

2. Select **Yes, restart** in the dialog box.
3. Log in when the login screen reappears.

Reboot Foundation appliances

If you encounter a serious error, you can reboot the Foundation base appliance by following instructions for rebooting virtual machines running on an ESX cluster (See VMware vSphere documentation) or by entering a command on the KVM management hypervisor. The Foundation base appliance cannot be rebooted from the CloudSystem Console.

Rebooting management appliances does not require rebooting compute nodes.

Reboot order

Reboot the associated Foundation and Enterprise appliances in the following order, if necessary.

1. SDN appliance
2. Network node appliances
3. vServer proxy appliance(s)
4. Enterprise appliance

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 8 Rebooting the Foundation base appliance on a KVM hypervisor

1. Log in to the management hypervisor on which the Foundation base appliance is running and enter the command:

   `virsh reboot` *`name_of_management_hypervisor`*
2. Open the CloudSystem Console in your browser, then log in.
3. If a login screen does not appear, enter the following commands on the management hypervisor:

   `virsh shutdown` *`name_of_management_hypervisor`*

   `virsh start` *`name_of_management_hypervisor`*
4. Optional. Create a support dump and send it to HP, which will help in diagnosing the problem and improving the product.

Update Foundation appliances

Use these procedures to install updates for Foundation appliances. To install updates on the Enterprise appliance, see Update the Enterprise appliance (page 130).

One large update image file (`*.bin`) updates one or more of these appliances:

- Foundation base appliance
- SDN controller
- Network nodes
- Proxy appliance
- Compute nodes

NOTE: When compute node updates are included in an image, CloudSystem components installed on KVM compute nodes are automatically updated. You need to install updates to RHEL distributions on KVM compute nodes separately. You must also install updates to vSphere or ESX on VMware compute nodes separately.

The time required for the download depends on the content delivered in the image file and the speed of your network connection.

IMPORTANT: When the update begins, non-critical services on all appliances (not just those being updated) are stopped, including HP Operations Orchestration. (Operations Orchestration work flows are not accessible during the update.) Critical services, such as the database and update services, are not stopped. If the update installation fails, the appliances revert back to their previous states and are restarted. Although CloudSystem services stop and restart, the physical systems hosting the compute nodes are not affected.

Prerequisites

- Minimum required privileges: Infrastructure administrator.
- HP recommends that you create and download a backup file before updating the appliances. Information about backing up and restoring HP CloudSystem is provided in a white paper available at Enterprise Information Library.

Procedure 9 Updating the Foundation appliances: Downloading the update file to your local computer

1. From the main menu, select **Settings**.
2. Select **Actions→Update Foundation appliances**.

   The **Update Foundation Appliances** screen is displayed.
3. Determine if other users are listed on the **Update Foundation Appliances** screen as currently logged in to the base appliance and, if necessary, inform them of the pending update.
4. Click "updates" in the line that reads "Go to hp.com for latest updates".
5. Locate the CloudSystem images for the appliance. Update images are encrypted files with a `.bin` extension.
6. Download the new image file to your local computer.

IMPORTANT: Once you have downloaded the file to your local computer, ensure there are no validation errors showing on the **Update Foundation Appliances** screen.

You are now ready to do one of the following.

- Upload the update file and install it at a later time.
- Upload the update file and install it immediately.

Procedure 10 Updating the Foundation appliances: Uploading an update file and installing it at a later time

You must have at least 2 GB of space available on the base appliance before proceeding.

1. To move the image file to the base appliance, do one of the following:
   - Drag the image file from a folder on your local computer and drop it in the box on the **Update Foundation Appliances** screen.

     NOTE: Some versions of Microsoft Internet Explorer do not support this method.
   - Click **Browse**, browse to the image file, and select it.
2. Click **Upload only**.

   The base appliance validates the image, and details of the pending update are displayed on the **Update Foundation Appliances** screen.

   If the image file is invalid, or if there is insufficient disk space, the appliance deletes the image file and displays the errors. Errors are also saved in `/updatelogs/update.log`. To download a new image file, see Downloading the update file to your local computer.

3. Once you are ready to install an uploaded image file:
   a. Return to the **Update Foundation Appliances** screen. (**Settings→Actions→Update Foundation appliances**).
   b. Examine the "File" name line.

      If the image you previously uploaded is not listed, then browse to select it.
   c. Proceed with step 2 in Uploading and installing an update file immediately.

Procedure 11 Updating the Foundation appliances: Uploading and installing an update file immediately

1. To move the image file to the base appliance, do one of the following:
   - Drag the image file from a folder on your local computer and drop it in the box on the **Update Foundation Appliances** screen.

     NOTE: Some versions of Microsoft Internet Explorer do not support this method.

     Click **Browse**, browse to the image file, and select it.
2. Click **Upload and install**.

   If this is the first time the image is being uploaded, the base appliance validates the image and details of the pending update are displayed on the **Update Foundation Appliances** screen.

   If the image file is invalid, or if there is insufficient disk space, the appliance deletes the image file and displays the errors. Errors are also saved in `/updatelogs/update.log`. To download a new image file, see Downloading the update file to your local computer.
3. Follow the "Release notes" link and read them to ensure that you understand the requirements of the update.

   NOTE: Save the *Release Notes* for future reference because when the download starts you will not be able to access the *Release Notes*.
4. Click **Continue**.

   The **CloudSystem Console License** screen appears.
5. To accept the license, click **Agree**.

   The **Update Foundation Appliances** screen is displayed.
6. Click **OK**.

   CloudSystem services are stopped, the console is locked, and progress of the upgrade is displayed on a status screen. When the update process completes, the Foundation base appliance restarts, and services on all appliances restart.

   Depending on the components in the update, the appliances might automatically reboot when the update is complete.
7. When the update completes and the console displays the login screen, log in and verify the new CloudSystem version information on the **Settings** screen. You can also navigate to the Activity screen from the main menu to check appliance statuses after the update.

Disassemble a CloudSystem installation

You can disassemble a CloudSystem installation when it is no longer needed.

IMPORTANT: The tasks you complete to disassemble a CloudSystem installation depend upon your business requirements for reusing the CloudSystem components. It is important that you select the correct procedure and complete the steps that are appropriate for your requirements.

- Disassembling a CloudSystem installation to reuse the underlying physical infrastructure (page 51).
- Disassembling a CloudSystem installation without removing the management cluster or hypervisor (page 51).

Procedure 12 Disassembling a CloudSystem installation to reuse the underlying physical infrastructure

Complete the following tasks if you do not want to use the management cluster or hypervisor.

1. Delete the virtual machine instances in the cloud. See Delete instance (page 109).
2. Power down and re-image the physical server.

Procedure 13 Disassembling a CloudSystem installation without removing the management cluster or hypervisor

Complete the following tasks if you want to continue using the management cluster or hypervisor.

1. Delete the virtual machine instances in the cloud. See Delete instance (page 109).
2. Detach the volumes attached to the virtual machine instances in the cloud. See Managing Volumes (page 93).
3. Deactivate the compute nodes in the cloud. See Deactivate a compute node (page 106).

NOTE: You do not need to delete the private networks.

4. Select and delete the appliance virtual machines that comprise CloudSystem.

NOTE: Delete the base appliance last in case you need to list the VMs again.

   a. Use the `csadmin appliances list` command to list all VMs that are managing the CloudSystem cloud. For example:

```
csadmin appliance list --os-username adminuser --os-password adminpassword --os-auth-url 10.x.x.x
-insecure
```

   b. Delete each appliance virtual machine in the list.
      - For a CloudSystem installation running in an ESX cluster, use VMware vCenter Server to select and delete the VMs.
      - For a CloudSystem installation running in a KVM hypervisor:
        a. If you are using an HA configuration, locate the name of the hypervisor where the appliance virtual machine is currently running.
        b. Enter the following OpenStack commands for each VM. Specify the `<vm_name>` for each appliance VM instance to remove from the management hypervisor:
           i. `virsh destroy <vm_name>`
           ii. `virsh undefined <vm_name>`
           iii. `rm /CloudSystem/images/<vm_name>.xml`
           iv. `rm /CloudSystem/images/<vm_name>.qcow2`
           v. After you delete the base appliance VM, enter `rm /CloudSystem/images/<vm_name>-glance.qcow2`. Specify the `<vm_name>` of the base appliance.

8 Manage users and groups

Use the information in this chapter to learn how to configure user authentication, either locally or using an enterprise directory, and to define user privileges based on job responsibilities, or role, in using this software. See also Troubleshooting users and groups (page 146).

About user roles

User roles enable you to assign permissions and privileges to users based on their job responsibilities. You can assign full privileges to a user, or you can assign a subset of permissions to view, create, edit, or remove resources managed by the appliance.

NOTE: If you are using an external authentication directory service such as LDAP in the CloudSystem Console, the role assignment is made to the group, rather than to individual users. However, in the CloudSystem Portal, roles are assigned to users per project, and groups are not recognized.

See the *HP CloudSystem 8.0 Release Notes* for information and limitations when mapping roles in the CloudSystem Console to the CloudSystem Portal. This document is available at the Enterprise Information Library.

Table 3 Appliance and resource management roles

Role	Type of user	Associated permissions or privileges	Notes
Full	**Infrastructure administrator**	View, create, edit, or remove resources managed by the appliance, including management of the appliance itself through the UI or command line. An Infrastructure administrator can also manage information provided by the appliance in the form of activities, notifications, and logs. An Infrastructure administrator can add CloudSystem Foundation license keys.	An *Infrastructure administrator* (Full role) created in the CloudSystem Console can view and manage all resources in the CloudSystem Console. Using the same username and password, the Infrastructure administrator can log into the CloudSystem Portal in the Admin role, with full access to the Administrator project. See also Table 4 (page 53).
Read only	**Read only**	View only access, with the exception of license keys. Users with this role see a message that they are not authorized to view license information.	A *Read only user* created in the CloudSystem Console can view all resources in the CloudSystem Console but cannot create, edit, or delete resources. A Read only user can log into the CloudSystem Portal if the user is a member or admin of a non-Administrator project. A Read only user is not restricted to Read only privileges in the CloudSystem Portal. This user has either full member or full administrator privileges depending on their user configuration in the CloudSystem Portal .
Specialized	**Backup administrator**	**NOTE:** Users with this role cannot log into the CloudSystem Console or CloudSystem Portal user interface.	No backup functions are provided in the CloudSystem Console. Information about backing up and restoring CloudSystem Foundation is provided in a white paper available at Enterprise Information Library.

Table 4 CloudSystem Portal roles

Role	Type of user	Associated permissions or privileges	Notes
Admin	**Cloud administrator**	View the **Admin** tab in the CloudSystem Portal. Administrative users can view usage and manage instances, volumes, flavors, images, projects, users, services, and quotas. For more information, see the *OpenStack Admin User Guide* at OpenStack Cloud Software.	A *Cloud administrator* created in the CloudSystem Portal can view and manage all resources in the CloudSystem Portal. The Cloud administrator can log into the CloudSystem Console only if he or she has a user account in the CloudSystem Console.
Member	**Cloud user**	View the **Project** tab in the CloudSystem Portal. Users can view and manage resources in the project to which they are assigned. For more information, see the *HP CloudSystem 8.0 Administrator Guide* at the Enterprise Information Library and the *OpenStack End User Guide* at OpenStack Cloud Software.	A *member* created in the CloudSystem Portal can view all services available to them in the CloudSystem Portal and can create, edit, and delete resources provided by those services. The actions a member can perform on their cloud are a subset of the actions an administrator can perform. A member user can log into the CloudSystem Console only if the user also has a user account in the CloudSystem Console.

Add a fully authorized local user (Infrastructure administrator)

Use this procedure to add a user with access to all resources, when your appliance authentication configuration is set to `LOCAL`.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- You must have the following information:
  - User's unique identifier name *(user_name)*
  - Initial password
  - User's full name
  - Optional: Contact information for the user

Procedure 14 Adding a fully authorized local user (Infrastructure administrator)

1. From the main menu, select **Users and Groups**→**Actions**→**Add**, or click **+ Add user** from the **Users and Groups** screen.
2. Enter the data requested on the screen. For information, click **Help on this page** in the CloudSystem Console.
3. Select Infrastructure administrator to assign the role with full access privileges to this user.
4. Click **Add** to create the user account, or click **Add +** to add another user.
5. Click **Close**.

   The user you added appears in the master list of users. Select the new user to view the account information.

About directory service authentication

You can use an external authentication directory service (also called an enterprise directory or authentication login domain) to provide a single sign-on for groups of users instead of maintaining individual local login accounts. An example of an authentication directory service is a corporate directory that uses LDAP (Lightweight Directory Access Protocol).

After the directory service is configured, any user in the group can log in to the appliance. On the login window, the user:

- Enters their user name (typically, the Common-Name attribute, CN).
- Enters their password.
- Selects the authentication directory service. This box appears only if you have added an authentication directory service to the appliance.

NOTE: If you are using an external authentication directory service:

- In the CloudSystem Console, the role assignment (for example, Infrastructure administrator) is made to the group, rather than to individual users.
- In the CloudSystem Portal, roles are assigned to users per project, and groups are not recognized.

IMPORTANT: The CloudSystem Portal is configured automatically based on the default directory set in the CloudSystem Console. You must set a default directory. See Set an authentication directory service as the default directory (page 60)

In the Session control, ( ) the user is identified by their name preceded by the authentication directory service. For example:

```
CorpDir\pat
```

Authenticating users

When you add an authentication directory service to the appliance, you provide search criteria so that the appliance can find the group by its DN (Distinguished Name). For example, the following attribute values identify a group of administrators in a Microsoft Active Directory:

```
distinguishedName      CN=Administrator,CN=Users,DC=example,DC=com
```

To authenticate a user, CloudSystem appends the user name to the search criteria and sends the authentication request to the configured LDAP or Active Directory service.

In the CloudSystem Portal, authorization data, including the members and administrators of a project, is associated with the user name. Authorization data does not include the search criteria or directory service. This means that changing the search criteria or default directory in the CloudSystem Console can allow CloudSystem Portal users to view and change resources in projects for which they are not authorized.

IMPORTANT: When changing the default directory or search context in the CloudSystem Console, ensure that the original and new directories or search criteria do not use the same user name to identify different individuals. For example, `smith.lab.users.example1.com`, `smith.marketing.users.example1.com`, and `smith.marketing.users.example2.com` are all authenticated as the user name `smith`.

Adding a directory server

After configuring and adding a directory server, you can designate it as the default directory service.

After you add an authentication directory service and server

You can:

- Allow local logins only, which is the default.
- Allow both local logins and logins for user accounts authenticated by the directory service.
- Disable local logins so that only users whose accounts are authenticated by the directory service can log in. Local accounts are prevented from logging in.

  HP does not recommend disabling local logins. If you disable local logins, Infrastructure administrator users that are not part of a directory group cannot log into the CloudSystem Portal.

Configuring CloudSystem to use Active Directory or OpenLDAP directory authentication

If you want to use directory service authentication instead of the default local login to authenticate users, you must first configure OpenLDAP or Microsoft Active Directory in the CloudSystem Console.

User authentication directories based on Lightweight Directory Access Protocol (LDAP) are used by CloudSystem to:

- Authenticate a user's login to the CloudSystem Console and CloudSystem Portal
- Authenticate a user's access to information

When a user logs in to the CloudSystem Console or CloudSystem Portal, LDAP authenticates the login credentials by verifying that the user name and password match an existing user in the LDAP directory. The LDAP server that hosts the directory should already be configured.

To configure OpenLDAP or Active Directory in the CloudSystem Console, perform the following configuration steps.

Add a directory service

A directory service contains a set of entries representing users. Each entry has a unique identifier: its **Distinguished Name (DN)**. The DN is constructed internally using the data you entered in the **search context** fields on the Add Directory screen and the user name.

The distinguished name is defined by the following:

- CN (common name) or UID (user identifier)

  Usually, the CN attribute identifies the user or group.
- OU (organizational unit) or CN (common name)
- DC (domain component)

The search context is the starting location that the authentication directory service uses to find users in its database.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The authentication directory service must be configured, and must accept SSL connections.
- You have obtained an X509 certificate from the directory service provider. This certificate ensures the integrity of communication between the appliance and the directory service.

Procedure 15 Adding an authentication directory service

1. From the main menu, select **Settings**.
2. Click the **Edit** icon in the **Security** area.
3. On the **Edit Security** screen, under **Directories**, click **Add Directory**.

4. Enter the data requested on the screen. See Editing Active Directory search context (page 56) or Editing OpenLDAP search context (page 57) for more information.
5. Click **Add** to add the authentication directory service or click **Add+** to add more directory services.

Determining search context when editing a directory

To specify the search context on the **Edit Security** screen, it it helpful to know some details about the internal structure of the LDAP server.

Browsing the LDAP server using an open source client can help you determine the search context, as shown in the following figures.

Editing Active Directory search context

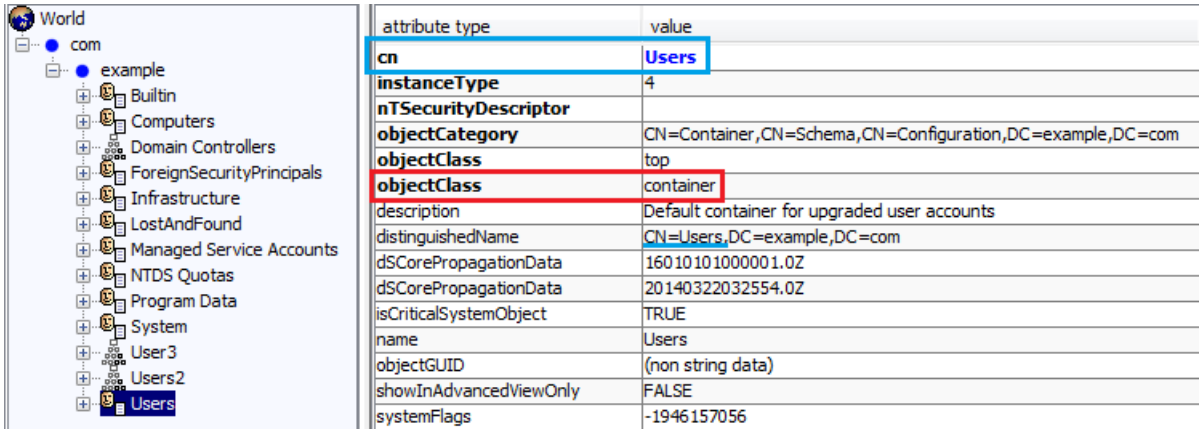
What should I specify for the *user identifier* (first text box) in the search context?

Typically, CN (common name) is the user identifier in Active Directory. Specify `CN`.

What should I specify for the *user search base* (second text box) in the search context?

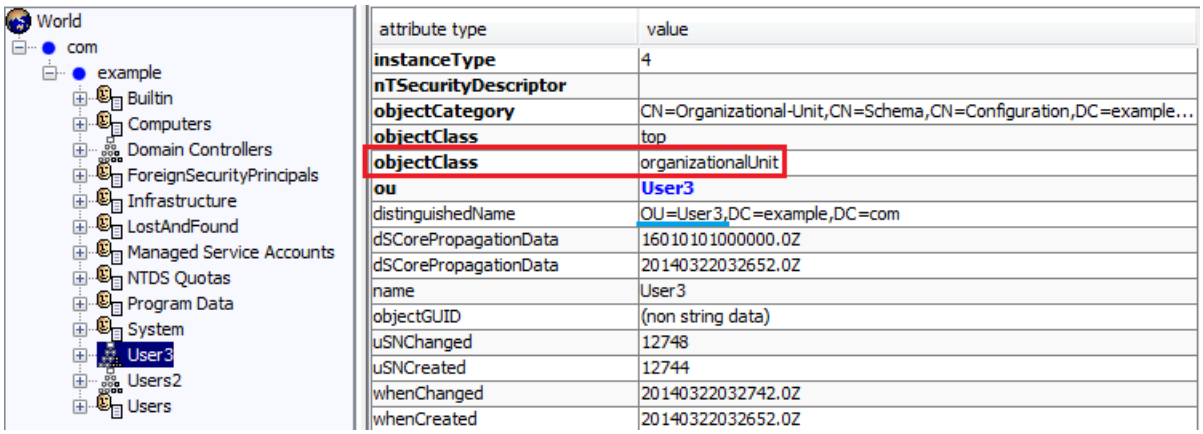
The following figure shows the "Users" branch of an Active Directory server. "Users" is a container, so in this example, you specify `CN=Users`.

Figure 7 User search base: `CN=Users`



The following figure shows the "Users3" branch of an Active Directory server. "Users3" is an OU (organizational unit). In this example, you specify `OU=Users3`.

Figure 8 User search base: `OU=Users3`



What should I specify for the *Base DN* (third text box) in the search context?

Specify the domain label and domain in which the user is authenticated. For example, for `smith.lab.users.example.com`, specify `DC=example, DC=com`.

Complete Active Directory search context

For a single search context where the users and a group reside in `CN=Users` and the DN is: `CN=Administrator, CN=Users, DC=example, DC=com`, enter it as follows:

First text box (User identifier)	Second text box (User search base)	Third text box (Base DN)
`CN`	`CN=Users`	`DC=example, DC=com`

Editing OpenLDAP search context

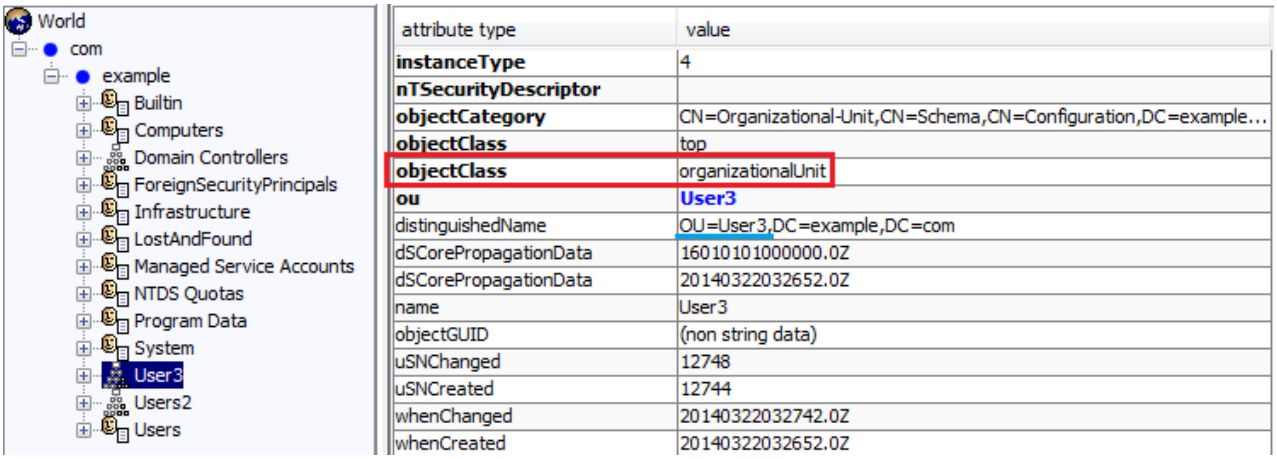
What should I specify for the *user identifier* (first text box) in the search context?

Typically, CN (common name) is the user identifier in OpenLDAP. Specify `CN`.

What should I specify for the *user search base* (second text box) in the search context?

The following figure shows the "Users" branch of an OpenLDAP server. "Users" is an OU (organizational unit). In this example, you specify `OU=users`.

Figure 9 User search base: `OU=Users`



What should I specify for the *Base DN* (third text box) in the search context?

Specify the Base DN (also known as the domain suffix). This is the domain in which the user is authenticated. For example, for `smith.lab.users.example.com`, specify `DC=example, DC=com`.

Complete OpenLDAP search context

For a single search context where the users reside in the container `OU=Users`, a group resides in the container `OU=Groups`, and the DN is: `CN=Administrator, OU=Groups, DC=example, DC=com`, enter it as follows:

First text box (User identifier)	Second text box (User search base)	Third text box (Base DN)
`CN`	`OU=Users`	`DC=example, DC=com`

Limitations: Directory tree

- **Active Directory**: Groups must be located under the user search base. Following are two examples:

  `CN=Users`

  `OU=US,OU=Users,OU=Accounts`

- **OpenLDAP**: Groups must be located under OU=Groups from the Base DN.

Limitations: Directory schema

An LDAP schema is a set of definitions and constraints about the structure of the directory information tree.

Table 5 Limitations on user and group object classes in LDAP

Directory service	User can log in to:	To log in, user enters:	Supported LDAP schema object classes for users	Supported LDAP schema object classes for groups

Active Directory	CloudSystem Console	User name, password, and directory	N/A	One of the following:
				`group`
				`groupOfNames`

Active Directory	CloudSystem Portal	User name and password
		NOTE: Users in authorized groups of the *default directory* can log in to the CloudSystem Portal.
			`user`	One of the following:
				`group`
				`groupOfNames`

OpenLDAP	CloudSystem Console	User name, password, and directory	N/A	`groupOfNames`
OpenLDAP	CloudSystem Portal	User name and password	`inetOrgPerson`	`groupOfNames`

Add a directory server

After you have added a directory *service*, you add the directory *server*. The directory server is the physical or virtual machine that hosts the authentication directory service.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The authentication directory service must be configured, and must accept SSL connections.
- You have obtained an X509 certificate from the directory service provider. This certificate ensures the integrity of communication between the appliance and the directory service.

IMPORTANT: By default, the CloudSystem Console and CloudSystem Portal do not perform strong LDAP server certificate validation. See Enabling strong certificate validation in the CloudSystem Portal (page 189) for the steps you can perform to require a valid client CA certificate chain when an OpenLDAP or Microsoft Active Directory service is used for authentication.

You can enable strong LDAP server certificate validation in the CloudSystem Portal only.

Procedure 16 Adding an authentication directory server

1. From the main menu, select **Settings**.
2. Click the **Edit** icon in the **Security** area.
3. On the **Edit Security** screen, under **Directories**, click **Add Directory**.

4. Click **Add a directory server**.
5. Enter the data requested on the screen. Click "Help on this page" in the CloudSystem Console for more information.
   a. Specify the host name (not the IP address) of the directory server, and the server port number.

      The port is used to communicate with the LDAP server using the LDAPS protocol. The default port for LDAP over SSL is 636.

   b. Obtain the directory server certificate. Enter the following command:

      `openssl s_client –host <directory-server-FQDN> -port 636`

      NOTE: If you are using a load-balanced (round robin) solution for your directory server, obtain the FQDN of one node in the server by entering the following commands.

      `nslookup <directory-server-FQDN>`

      A list of IP addresses is returned. Select one IP address and enter:

      `nslookup <directory-server-IP address>`

      Enter the FQDN returned for this IP address as the `<directory-server-FQDN>` in the `openssl` command above.

   c. Copy the X509 certificate for the server and paste it into the box on the screen.
6. Click **Add** to add the server and return to the **Add Directory** screen.

Add a directory group

You add a directory group that exists in the authentication directory service by which users will be authenticated through the directory service. You assign the group full access to resources or a subset of resources based on job responsibilities.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The group exists in the authentication directory service.
- You know the credentials of a directory service user.

  The appliance uses these credentials to confirm the user's permission to access it. The credentials are not saved on the appliance.
- The directory service must be added to the appliance. For more information, see Add a directory service (page 55).

Procedure 17 Adding a group with directory-based authentication

1. From the main menu, select **Users and Groups→Actions→Add Directory Group**.
2. Enter the data requested on the screen. Click "Help on this page" in the CloudSystem Console for more information.
   a. Select the authentication directory service.
   b. Enter the credentials to log in to the directory service.
   c. Click **Connect**.

      You can use the same credentials that you specified on the **Add Directory** screen. You can also use different credentials, if desired.

   d. Select the group from the menu.

e. Select the role.

The role assignment specifies the permission level for all users in the group. See About user roles (page 52) for more information.

NOTE: If you are using an external authentication directory service, in the CloudSystem Console, the role assignment is made to the group rather than to individual users. Therefore, all users in a group who log in to the CloudSystem Console have the same role assignment (for example, Full or Read only). However, in the CloudSystem Portal, roles are assigned to users per project, and groups are not recognized. Users who log in to the CloudSystem Portal can have different roles (for example, Admin or Member).

3. Click **Add** to add the group and return to the **Users and Groups** screen, or click **Add+** to add another group.

Set an authentication directory service as the default directory

Initially, the default directory is the local directory of user accounts.

- You can designate an authentication directory service as the default directory.

IMPORTANT: You must set a default directory. Only users in authorized groups of the *default directory* can log in to the CloudSystem Portal.

Setting a default directory enables directory service authentication. See Setting an authentication directory service as the default directory (page 60).

- If you added more than one authentication directory service, you can select a directory as the default directory.

On the CloudSystem Console login screen, you see the names of all configured directories under the user name and password boxes. When you log in, you select the directory. The default directory is at the top of the list and is selected by default.

On the CloudSystem Portal login screen, the user name and password boxes are displayed. CloudSystem automatically authenticates the user against the default directory.

IMPORTANT: If you configure more than one directory service, ensure that the directories do not use the same user name to identify different individuals. For example, `smith.lab.users.example1.com`, `smith.marketing.users.example1.com`, and `smith.marketing.users.example2.com` are all authenticated as the user name `smith`.

If you have more than one directory that contains the same user name, changing the default directory in the CloudSystem Console can allow CloudSystem Portal users to view and change resources in projects for which they are not authorized. See About directory service authentication (page 53).

Prerequisites

- Minimum required privileges: Infrastructure administrator
- At least one authentication directory service must be available on the appliance. See Add a directory service (page 55).

Procedure 18 Setting an authentication directory service as the default directory

1. From the main menu, select **Settings**.
2. Click the **Edit** icon in the **Security** area.
3. Select an authentication directory service under **Directories** on the **Edit Security** screen.
4. Click **OK**.

Allow local logins

The appliance is configured to allow local logins by default.

If you disabled local logins so that you could use an authentication directory service exclusively, use this procedure to allow local logins.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 19 Allowing local logins

1. From the main menu, select **Settings**.
2. Click the **Edit** icon in the **Security** area.
3. Select the **Allow local login** check box on the **Edit Security** screen.
4. Click **OK**.

Disable local logins

If you want to authenticate all logins to the appliance through an authentication directory service, you must disable local logins.

The authentication directory service administrator must use the directory service to disable remote logins.

NOTE: Local logins cannot be disabled until you log in using an authentication directory service. HP recommends that you verify that you can log in to the appliance as an Infrastructure administrator from the authentication directory service before continuing.

HP does not recommend disabling local logins. If you disable local logins, Infrastructure administrator users that are not part of a directory group cannot log into the CloudSystem Portal.

Prerequisites

- Minimum required privileges: Infrastructure administrator.
- You must be logged in to the appliance from the authentication directory service.

Procedure 20 Disabling local logins

1. From the main menu, select **Settings**.
2. Click the **Edit** icon in the **Security** area.
3. Clear the **Allow local login** check box.
4. Click **OK**.

Reset the administrator password

If you lose or forget the administrator password to the Foundation base appliance, you can reset it from the base appliance with telephone assistance from your authorized support representative.

Prerequisites

- You have access to the appliance console.
- The appliance software is running.

Procedure 21 Resetting the administrator password

1. From the console appliance login screen, switch to the `pwreset` login screen by pressing **Ctrl+Alt+F1**. To return to the console's login screen, press **Ctrl+Alt+F2**.

   NOTE: For **VMware vSphere** users, **Ctrl+Alt** is used for another function. To send the command to the console, you must press **Ctrl+Alt+Spacebar** then press **Ctrl+Alt+F1**.

   For **KVM** users, to send the command to the console, you must select **Send Key→Ctrl+Alt+F1** menu item from the Virtual Machine Manager.

2. Log in with the user name `pwreset`.

   The appliance displays a challenge key. For example:

   ```
   <hostname> login: pwreset
        Challenge = xyaay42a3a
        Password:
   ```

3. Telephone your authorized support representative and read the challenge key to them. They will provide you with a short-lived, one-time password based on the challenge key.

   For information on how to contact HP by telephone, see How to contact HP (page 41).

   The authorized support representative uses the challenge code to generate a short-lived, one-time password based on the challenge key. It will be an easy-to-type, space-separated set of strings. For example:

   ```
   VET ROME DUE HESS FAR GAS
   ```

4. Enter the password that you receive from your authorized support representative.

   The appliance generates a new password.

5. Note the new password for the administrator account, and then press **Enter** to log out.
6. Log in as administrator using the new password.

   The generated password expires immediately after use; you must create a new password.

9 Manage licenses

You can manage licenses from the CloudSystem Console. Use the information in this chapter to manage and track your license compliance.

About licenses

CloudSystem software licensing is based on one of the following options, as recorded in the license terms in your purchase agreement.

- The number of active operating system instances (OSIs), or
- The number of servers in your cloud

  Server-based licenses allow you to use Matrix OE software to manage cloud services that are deployed across a specified set of licensed physical servers.

NOTE: The software license type you purchase enables you to manage your environment in different ways.

- *OSI licenses* allow a fixed number of virtual machine instances to be deployed on any server in a private, hybrid, or public cloud infrastructure.
- Server licenses allow an unlimited number of virtual machine instances to be deployed only on the licensed server.

You can add more licenses at any time to increase your OSI or server capacity.

Each CloudSystem software license includes rights to use the CloudSystem software to manage up to the licensed number of operating system instances or servers concurrently.

Refer to your license entitlement for the number of instances included in your standalone or solution license.

Before adding license keys, you can configure resources in CloudSystem Foundation and install CloudSystem Enterprise. Deploying and managing instances requires a license.

Rights to use HP OneView are *not* granted by the CloudSystem Foundation or Enterprise software license. While both CloudSystem and HP OneView are delivered as part of some CloudSystem solution offerings, HP OneView and CloudSystem are separate products, and are licensed independently under their respective license agreements.

CloudSystem Foundation Software

The CloudSystem Foundation software license also includes HP Operations Orchestration and HP Cloud OS.

To view CloudSystem Foundation license usage, on the CloudSystem Console **Settings** screen, select **Overview**, then **Licenses**. See View license details (page 66).

If you are logged in as an Infrastructure administrator, you can add CloudSystem Foundation license keys from the **Actions** menu on the **Settings** screen. See Add a license key to the appliance (page 65). For information about other user roles and licensing privileges, see About user roles (page 52).

CloudSystem Enterprise Software

NOTE: Use the Cloud Service Management Console in the Enterprise appliance to view, add, and remove HP CSA license keys. In the free trial period (the first 90 days), if you have not yet added a license key, HP CSA limits the number of new instances you can create.

To add HP CSA license keys, first install CloudSystem Enterprise from the CloudSystem Console Enterprise screen. Then click the link for HP CSA to launch the management console. From the **Options** menu, select **Licensing**.

CloudSystem Enterprise software is offered under a single license entitlement. All embedded technologies are licensed, sold, and supported together as a single, non-decomposable product. The Enterprise software license also includes rights to use the embedded Matrix Operating Environment (Matrix OE) software to manage an unlimited number of operating system instances on the specified number of servers.

The CloudSystem Enterprise software license includes:

- CloudSystem Foundation (including Operations Orchestration and Cloud OS)
- HP Cloud Service Automation
- HP Matrix Operating Environment
- HP Insight Control

Your per-OSI licensed environment must account for instances provisioned by all technologies. Instances provisioned or managed by both CloudSystem Foundation and CloudSystem Enterprise are counted only once.

Migrating your license to a new server

When you purchase a CloudSystem Enterprise per-OSI software license, you can transfer your rights to manage a server with Matrix OE (including Insight Control) to a replacement server. To migrate your license to a new server:

- Add the existing Matrix OE license key to the new server.
- Add the replacement Insight Control license key to the new server. (The replacement license key is included with the original license key when you purchase a CloudSystem Enterprise software license.)

For license support, see http://www.hp.com/software/licensing-support.

To read the license documents, see http://www8.hp.com/us/en/campaigns/prodserv/software-licensing.html.

License keys

License keys are required to enable the components of the purchased CloudSystem software product.

1. Activate your license(s) on http://www.hp.com/software/licensing to obtain license keys.
2. For CloudSystem Foundation licenses, add the license key to the Foundation appliance using the **Settings** screen. See Add a license key to the appliance (page 65).
3. For CloudSystem Enterprise licenses, add each license key to the corresponding management console that you plan to use. For example, add the Foundation license key to the Foundation

console, the Enterprise license key to the Cloud Service Management Console in the Enterprise appliance, and the Matrix OE license to the CMS.

- CloudSystem Foundation licenses include one key. This key enables the use of the CloudSystem Foundation appliance.
- CloudSystem Enterprise licenses include four or more keys. These keys enable the use of the following:
  - CloudSystem Foundation appliance
  - CloudSystem Enterprise appliance
  - Matrix Operating Environment CMS (Central Management Server)

    When you receive Matrix OE as part of CloudSystem Enterprise under a per-OSI license, you also receive rights to transfer your Matrix OE server license from one licensed physical server to a replacement server using your current server license key.
  - HP Insight Control

    When you receive Insight Control as part of CloudSystem Enterprise under a per-OSI license, your Insight Control server license key *cannot* be transferred to a replacement server. Use the server replacement license key to activate a replacement server.

Managing license compliance

You are accountable for sizing your license requirements and purchasing the number of licenses necessary to meet your needs. Because exceeding the number of licensed instances is possible, you should track your compliance and purchase additional licenses if you exceed your license limits. License compliance is subject to HP audit at any time.

Add a license key to the appliance

You can purchase and activate CloudSystem Foundation and CloudSystem Enterprise licenses and add license keys to the appliance. See About licenses (page 63).

Prerequisites

- Minimum required privileges: Infrastructure administrator
- You have at least one license key
- You activated and registered your new standalone licenses at the HP licensing portal:

  https://hp.com/software/licensing

Procedure 22 Adding a license key to the appliance

1. From the main menu, select **Settings**.
2. Select **Actions→Add license**.

   The **Add License** dialog box is displayed.
3. Enter or paste your license key in the **License Key** box and then either click **Add** to complete the action or click **Add +** to add another key.

   If the key is valid, it will be added to the appliance. If the key is not valid, you will be prompted to add a valid key.

License key format

The supported key format is:

<encrypted_key_string> "*<annotation>*"_*<optional_encrypted key_string>*

The encrypted key string is expected to be a series of character/number blocks separated by spaces. The annotation includes space separated fields representing an HP sales order number, a product number, a product description, and an EON (entitlement order number).

Example CloudSystem Foundation key:

ABKE C9MA T9PY 8HX2 V7B5 HWWB Y9JL KMPL K6ND 7D5U UVQW JH2E ADU6 H78V ENXG TXBA KFVS D5GM ELX7 DK2K HKK9 DXLD QRUF YQUE BMUF AQF2 M756 9GVQ QZWD LY9B V9ZF BG2B JKTG 2VCB LK4U R4UR V886 3C9X MQT3 G3AD LVKK 5LRG E2U7 GHA3"Order1 Number2 CloudSystem_Foundation_Example_License EON3"

View license details

From the **Settings** screen, select **Licenses** from the **View** menu.

The information on the **Licenses** screen applies to cloud environments enabled with CloudSystem per-OSI licenses. The information on this screen does not reflect per-server license compliance.

Table 6 License graph colors

Color	Description
Yellow	Percentage of operating system instances without a license
Blue	Percentage of operating system instances that are licensed
Light Gray	Licenses that are available but have not been assigned

Screen component	Description
Graph 	Identifies the product license and indicates: • The percentage of active instances that are licensed in CloudSystem Foundation under a per-OSI license. Hover your mouse over the graph to see the percentage of unlicensed instances, if any. • The number of currently licensed instances. • The highest number of instances in use at one time. If this number is higher than the number of licenses available, see Managing license compliance (page 65) for information about tracking your compliance. • The number of licenses available. If no product licenses are applied, `No licenses` is displayed with the **Add** button so that you can add a license.

10 Manage security

Primarily, securing CloudSystem appliances require attention to properly managing certificates. This chapter and Security in CloudSystem (page 22) provide guidance on using certificates in CloudSystem. See also Troubleshooting security settings (page 149).

Note that this software provides the ability to enable or disable service access. To learn more about this feature, see Enabling or disabling authorized services access (page 24)

Access to the appliance console

Use the hypervisor management software to restrict access to the appliance, which prevents unauthorized users from accessing the password reset and service access features. See Restricting console access (page 24).

Typical legitimate uses for access to the console are:

- Troubleshooting network configuration issues.
- Resetting an appliance administrator password.

  For information on how to reset the administrator password, see the online help.
- Enabling service access by an on-site authorized support representative.

The virtual appliance console is displayed in a graphical console; password reset and HP Services access use a non-graphical console.

Procedure 23 Switching from one console to another (VMware vSphere)

1. Open the virtual appliance console.
2. Press and hold **Ctrl+Alt**.
3. Press and release the space bar.
4. Press and release **F1** to select the non-graphical console or **F2** to select the graphical console.

Procedure 24 Switching from one console to another (KVM)

1. Open the Virtual Machine Manager.
2. In the Menu bar, select **Send Key→Ctrl+Alt+F1** for the non-graphical console or select **Send Key→Ctrl+Alt+F2** for the graphical console.

Downloading and importing a self-signed certificate

The advantage of downloading and importing a self-signed certificate is to circumvent the browser warning.

In a secure environment, it is never appropriate to download and import a self-signed certificate, unless you have validated the certificate and know and trust the specific appliance.

In a lower security environment, it might be acceptable to download and import the appliance certificate if you know and trust the certificate originator. However, HP does not recommend this practice.

Microsoft Internet Explorer and Google Chrome share a common certificate store. A certificate downloaded with Internet Explorer can be imported with Google Chrome as well as Internet Explorer. Likewise, a certificate downloaded with Google Chrome can also be imported by both browsers. Mozilla Firefox has its own certificate store, and must be downloaded and imported with that browser only.

The procedures for downloading and importing a self-signed certificate differ with each browser.

Procedure 25 Downloading a self-signed certificate with Microsoft Internet Explorer 9

1. Click in the **Certificate error** area.
2. Click **View certificate**.

3. Click the **Details** tab.
4. Verify the certificate.
5. Select **Copy to File...**
6. Use the Certificate Export Wizard to save the certificate as Base-64 encoded X.509 file.

Procedure 26 Importing a self-signed certificate with Microsoft Internet Explorer 9

1. Select **Tools**→**Internet Options**.
2. Click the **Content** tab.
3. Click **Certificates**.
4. Click **Import**.
5. Use the Certificate Import Wizard.
   a. When it prompts you for the certificate store, select **Place…**.
   b. Select the **Trusted Root Certification Authorities** store.

Verifying a certificate

You can verify the authenticity of the certificate by viewing it with your browser.

After logging in to the appliance, choose **Settings**→**Security** to view the certificate. Make note of these attributes for comparison:

- Fingerprints (especially)
- Names
- Serial number
- Validity dates

Compare this information to the certificate displayed by the browser, that is, when browsing from outside the appliance.

Part III Resource configuration in CloudSystem Foundation

11 Overview: Configuring compute resources

Use this part of the Administrator Guide to learn when and how to use the CloudSystem Foundation Console to configure, monitor and manage virtual compute resources. This chapter outlines a suggested order in which you can proceed and provides a table of maximum supported configuration values that you can use to plan your cloud size. The remaining chapters are organized primarily by compute resource category.

Configuring cloud resources

The virtualized resources that you can configure and manage in CloudSystem Foundation are shown in the following table.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The Data Center Management Network connects the 3PAR storage system, the vCenter Server, and/or the enclosure that contains the compute nodes with the CloudSystem management hypervisor.
- For ESX clusters, one or more vCenter Server s are registered in the CloudSystem Console on the **Integrated Tools** screen.

Configuring cloud resources in CloudSystem Console

☑	CloudSystem Foundation Task
	1. Add a Provider Network A Provider Network is part of the Cloud Data Trunk, which is the physical network hosting the VLANs that OpenStack networking makes available to users. The Cloud Data Trunk provides communication for compute nodes and virtual machine instances.
	2. Add one or more images An image is a template for a virtual machine file system. It contains information about the operating system to provision to a virtual machine instance.
	3. Add a block storage driver A block storage driver defines the characteristics of the volume type that is created for storage systems. Drivers deliver technology or vendor-specific implementations for the OpenStack Block Storage functionality. CloudSystem supports the 3PAR FC, Direct-Attach and iSCSI drivers. These drivers require connectivity to the management console of a supported HP 3PAR storage system.
	4. Add volume types A volume type describes the characteristics of a class of volumes that can be selectable by a cloud user. For the HP 3PAR drivers, each volume type is associated to a block storage driver and a Common Provisioning Group (CPG). The hypervisor type (KVM or ESX) is also defined in the volume type.
	5. Verify or add flavors Flavors define the size of compute resources (number of virtual CPUs, memory and ephemeral storage capacity) that can be assigned automatically to virtual machines.
	6. Create compute nodes You create and manage **ESX** compute hosts in vCenter Server. All compute hosts are configured as clusters. You impot these clusters into CloudSystem. You create **KVM** compute nodes on KVM hosts. After a KVM compute node is created, it appears on the Compute Node screen in the CloudSystem Console with an Unknown status, meaning it is not yet activated.
	7. Import ESX clusters CloudSystem retrieves information about an ESX cluster when you import it. The cluster is added to the Compute Nodes overview screen in an Unknown state, meaning it is not yet activated.
	8. Activate a compute node Your ESX cluster or KVM compute nodes must already be visible in the CloudSystem Console. Activating a KVM compute node installs OpenStack agents on the compute node. (Activating an ESX cluster does not install any software.) After activation, the ESX clusters or KVM compute nodes are ready to serve as targets for resource provisioning.

Maximum supported configuration values for each CloudSystem

Each instantiation of CloudSystem Foundation software supports a maximum of configured resources as shown in the following table.

Configured resource	Maximum number supported
Managed virtual machine instances	5,000
Managed hypervisor hosts	100
CloudSystem Portal users	32
CloudSystem Portal users simultaneously creating virtual machine instances	5

Configured resource	Maximum number supported
CloudSystem Portal users simultaneously configuring OpenStack non-storage operations (Nova, Neutron, Glance, and Keystone)	25
Projects	256
Virtual machine instances per project	500
Images	512
Flavors	32
External networks	1
Provider networks	32
Private IP addresses	5,000
Floating IP addresses	1,000
Private (tenant) networks	256
Disk arrays	2
Block storage volumes created	3,000
Block storage volumes attached	250
Block storage volumes per ESX cluster	256
Virtual machine instances belonging to a single security group	500
Clusters per vCenter Server	16
Nodes per ESX cluster	16
vCenter Servers	3

12 Network configuration

This chapter provides instructions for configuring the networks necessary to support the interoperability of the CloudSystem appliances and the virtualized resources in the cloud. You will need to use both the CloudSystem Console and the CloudSystem Portal to configure the networks. See also How it works (page 15).

About Cloud Networking

You complete the setup of the Foundation appliance by configuring the Cloud Management Network on the Cloud Networking pane of the Settings screen. When the settings are saved, the Foundation appliance automatically creates the Software Defined Network (SDN) controller and three network node appliances. Using three network nodes provides increased reliability and scalability. Each of these appliances runs in its own virtual machine. Creating these appliances can take 5 to 15 minutes to complete.

The Cloud Networking settings control the configuration of the private network that connects the CloudSystem Foundation base appliance to compute nodes and virtual appliances. See CloudSystem appliances and network infrastructure (page 16).

Cloud Management Network

After you configure Cloud Networking, the SDN controller runs in the background to manage CloudSystem Console network connections. The base appliance provides a DHCP service on the Cloud Management Network, and the network node appliances provide DHCP IP addresses for virtual machine deployment. The network nodes use only the Cloud Management Network you specify. They do not have public IP addresses.

NOTE: Verify that the management hypervisor can support the additional appliances that are created during cloud network setup.

Can I edit cloud networking after compute nodes are activated?

Cloud networking can be edited when there are no activated compute nodes. After compute nodes are activated, changing the cloud networking configuration requires resetting your environment.

If you must change the cloud networking configuration after compute nodes are activated, first perform the following tasks to reset your environment.

1. Back up any user data on virtual machine instances.
2. Delete virtual machine instances. See Delete instance (page 109).
3. Deactivate compute nodes. See Deactivate a compute node (page 106).
4. Then, edit the Cloud Management Network. See Edit Cloud Networking (page 73).

Edit Cloud Networking

Use this procedure to edit the Cloud Management Network.

IMPORTANT: Cloud networking is intended to be configured only once. Ensure that the cloud networking information you specify is accurate. After compute nodes are activated, changing the cloud networking configuration requires resetting your environment. See Can I edit cloud networking after compute nodes are activated? (page 73)

Prerequisites

- Minimum required privileges: Infrastructure Administrator
- No compute nodes are activated on the network.

Procedure 27 Editing a cloud network

1. From the main menu, select **Settings**.
2. Select **Edit Cloud Networking**, or click the **Edit** icon on the **Cloud Networking** pane.
3. Enter data. Click "Help on this page" in the CloudSystem Console for more information.
4. To save your edits, click **OK**.

   To exit the action with no change made to the network, click **Cancel**.
5. Verify that the updated setting information is displayed in the **Settings→Cloud Networking** pane.

About Provider Networks

A Provider Network is a shared network in the data center on which users can provision virtual machine instances. Adding a Provider Network enables you to add an existing data center network to virtual machine instances in the cloud.

Provider networks in the cloud

A Provider Network is part of the Cloud Data Trunk, which is the physical network hosting the VLANs that OpenStack Networking makes available to users. The Cloud Data Trunk connects compute nodes and allows virtual machine instances to communicate with each other. Private Networks are also part of the Cloud Data Trunk.

Once created, provider networks are shared by all projects in the CloudSystem.

Managing provider networks

Once you add a Provider Network, you can use the CloudSystem Console to manage the network. You can also use the OpenStack Networking API or CLI to manage the network.

You can use the Dashboard to track the number of Provider Network IP addresses that are assigned to instances. See the Network section in Interpreting the Dashboard data.

NOTE: The OpenStack Networking service assigns a unique identifier (ID) to each Provider Network. The service uses the ID to differentiate each network. Because you can create more than one network with the same name, but with different IDs, you might want to specify a unique name for each Provider Network so that you can easily differentiate between networks.

Add Provider Network

Adding a Provider Network enables you to provision an existing data center network to the cloud.

Prerequisites

- Minimum required privileges: Infrastructure Administrator
- Cloud Networking is configured.

Procedure 28 Adding a Provider Network

1. From the main menu, select **Provider Networks**.
2. Click **+ Add Network**.
3. On the **Add Provider Network** screen, enter a **Name** and **VLAN ID** for this network.
4. If you do not want this network to be shared by other components, such as virtual machines and hypervisors, clear the **Shared** check box.
5. If you do not want this network to forward packets, clear the **Admin State Up** check box.
6. Optional: To add a subnet to this network, do one of the following.
   - To add a subnet to a new network:
     1. Click **Add subnet**.

2. On the **Add Subnet** screen, enter an IPv4 address in CIDR format to specify the IP address range available to this network.
3. If the IP addresses listed for **Allocation Pools** or **Gateway IP** are not correct, change the default values.
4. If the network already has a DHCP server, clear the **Enable DHCP** check box.
5. Click **OK**.
6. Verify that the new subnet is displayed on the **Add Provider Network** screen. To sort by CIDR, select the **CIDR** column heading.

- To add a subnet to an existing network:
  1. On the **Provider Networks** overview screen, select the row of the network to which you want to add a subnet.
  2. Select **Actions→Edit**.

     Alternatively, hover over the details of the selected network to display the **Edit** icon, and then click the **Edit** icon.
  3. On the **Add Subnet** screen, enter an IPv4 address in CIDR format to specify the IP address range available to this network.
  4. If the IP addresses listed for **Allocation Pools** or **Gateway IP** are not correct, change the default values.
  5. If the network already has a DHCP server, clear the **Enable DHCP** check box.
  6. Click **OK.**
  7. Verify that the network update was successful by reviewing the fields on the **Edit Provider Networks** screen. To sort by CIDR, select the **CIDR** column heading.

7. Finish adding the network.
   - To add only this network, click **Add**.

     The new network displays on the overview screen.
   - To add more than one network:
     1. Click **Add+** to complete the addition process for the first network and reset the form.

        The **Name** and **VLAN ID** fields are cleared, but the other options remain checked for future use.
     2. Enter a unique **Name** and **VLAN ID** for the network.
     3. Update other options if needed.
     4. Repeat steps 1, 2, and 3 until you are finished adding additional networks, then click **Cancel** to dismiss the **Add Provider Network** screen.
8. Verify that each new network is displayed on the **Provider Networks** screen. To sort by network name, select the **Name** column heading.

Delete Provider Network

Use this procedure to delete a Provider Network and its associated subnets. Upon deletion, the network and its associated subnets are no longer available in the cloud.

Prerequisites

- Minimum required privileges: Infrastructure Administrator
- A VM instance or router is not assigned an IP address on the network to be deleted.

Procedure 29 Deleting a Provider Network

1. From the main menu, select **Provider Networks**.
2. Select the row of the network to be deleted.
3. Select **Actions→Delete**.

4. On the **Delete Provider Network** screen, click **Yes, delete**.
5. Verify the network deletion by reviewing the fields on the **Provider Networks** screen.

About Private Networks

Private Networks are created from a pool of VLANs, which you configure using the CloudSystem Console. The OpenStack Networking service assigns VLANs from this pool to Private Networks when they are created by end users using the CloudSystem Portal.

End users create Private Networks to associate with their provisioned virtual machine instances. End users can assign Private Networks to virtual machine instances during virtual machine provisioning.

Private Networks in the cloud

Private Networks are part of the Cloud Data Trunk. End users create individual Private Networks using VLANs that you identify for that purpose. Therefore, each Private Network is shared exclusively among members of a given project. See also How it works (page 15).

Managing private networks

Using the CloudSystem Console, you can select which VLANs are available for provisioning to private networks. Once you add a private network VLAN, you can also use the console to delete VLAN IDs, removing them from the pool of VLANs available for private network assignment.

End users use the CloudSystem Portal to create new private networks mapped to available VLANs, and to manage their private network topologies. When a user configures a private network in the CloudSystem Portal, the OpenStack Networking service assigns a VLAN ID from the VLAN IDs configured for that project. The user does not explicitly specify the VLAN ID for a private network.

You can also use the Dashboard to track the number of private network IP addresses that are assigned to instances. See the Network section in Interpreting the Dashboard data.

Understanding private networks data

Select at least one VLAN to display data on the overview screen. When you select more than one VLAN, your selections are highlighted in the list, the total number of networks selected is displayed at the top of the overview screen, and detailed data for each network is displayed underneath.

The Dashboard also displays data about private networks. See the Network section in Interpreting the Dashboard data.

Add VLAN IDs

Use this procedure to add VLAN IDs to the pool of VLANs available for Private Network assignments. End users can then use the CloudSystem Portal to create Private Networks from these assignable VLAN IDs.

Prerequisites

- Minimum required privileges: Infrastructure Administrator
- A pool of VLANs is created in the cloud and the VLANs are not yet allocated.

Procedure 30 Adding VLAN IDs for use in Private Networks

1. From the main menu, select **Private Networks**.
2. Click **+Add VLAN**.
3. List the VLAN IDs or VLAN ID ranges separated by commas in the box provided.
4. Click **Add**.
5. Verify that the new VLAN IDs are listed on the **Private Networks** overview screen.

Delete Private Network VLAN

Use this procedure to delete unassigned Private Network VLANs. After you delete a VLAN, it cannot be assigned to a Private Network.

Prerequisites

- Minimum required privileges: Infrastructure Administrator
- The VLAN status must be **unassigned**.

Procedure 31 Deleting a Private Network VLAN

1. From the main menu, select **Private Networks**.
2. Select one or more unassigned VLANs to be deleted.
3. Select **Actions→Delete**.
4. On the **Delete VLANs** screen, click **Yes, delete**.
5. With the filter set to **All assignments**, verify that the private network VLAN no longer appears on the **Private Network** overview screen.

About the External Network

The External Network allows you to route virtual machine instances on Private networks out from the CloudSystem private cloud to the data center, the corporate intranet, and the internet.

One External Network is automatically created during CloudSystem Foundation installation. Virtual machines are not directly attached to the External Network. Internal Provider and Private networks connect directly to virtual machine instances. The External Network connects to network nodes.

After installation, you can use the features in the CloudSystem Portal to enable use of the External Network for accessing VM instances on cloud networks. You create a subnet for the External Network. Cloud users can then create routers to connect the External Network to Private networks for their projects. Traffic from the External Network is routed to selected virtual machines inside the cloud using floating IP addresses.

Because a single subnet is allowed for the External Network, you should configure one that is large enough to accommodate future expansion.

Configuring the External Network

To configure the External Network for use in routing traffic to selected virtual machines inside the cloud, complete the following procedures:

1. Creating the External Network subnet (page 78)
2. Creating a router to connect Private Network instances to the External Network subnet (page 79)
3. Assigning floating IP addresses to instances (page 79)

Creating the External Network subnet

Creating an External Network subnet enables the network nodes to route traffic from the subnet so that cloud users can access virtual machine instances on Private networks. Use this procedure to create a subnet.

IMPORTANT:

- Cloud users should never select the External Network when creating virtual machine instances.
- Do not edit the name, ID, or administrative state of the External Network that is automatically set during CloudSystem Foundation installation.
- Do not delete the External Network that is automatically created during CloudSystem Foundation installation. (See External Network information is not listed on the CloudSystem Portal (page 157).)
- Because you create a single subnet for the External Network, you should configure one that is large enough to accommodate future expansion.

Prerequisite

- Minimum required privileges: Infrastructure administrator

Procedure 32 Creating the External Network subnet

1. Log on to the CloudSystem Portal.
   a. Append **/portal** to the Foundation appliance URL in your browser (for example, `https://192.0.2.0/portal`).
   b. Enter your user name and password, and then click **Sign In**.
2. From the **Admin** tab, in the "System Panel" section, select **Networks**.
   The **Network** screen opens and displays a list of configured networks.
3. Click the **External Network** link.
   External Network details appear on the **Network Overview** screen.
4. On the right side of the "Subnets" section, click **+ Create Subnet**.
   The **Create Subnets** screen opens with the **Subnet** tab selected.
5. Complete the **Subnet** tab settings.
   - **Subnet Name**—Enter a unique name for the subnet. A maximum of 255 alphanumeric characters is allowed.
   - **Network Address**—Enter an IPv4 address in CIDR format specifying the IP address range to use for the subnet.
   - **IP Version**—Leave the default setting at **IPv4**.
   - **Gateway IP**—Enter the IPv4 address of the router providing access to this subnet.
   - **Disable Gateway**—Leave this check box cleared to allow the router to access networks inside the cloud.
6. Select the **Subnet Detail** tab and complete these settings:
   - **Enable DHCP**—Click the check box to clear this option, allowing the use of floating IPs for routing traffic.
   - **Allocation Pools**—Enter the IP address ranges to make available for floating IP address assignment on the subnet.
7. Click **Create**.
   Details about the External Network subnet are displayed on the **Network Overview** screen.

Cloud users should now be able to create routers to connect the External Network subnet to Private networks for their projects. You can verify that a router can be connected. See Creating a router to connect Private Network instances to the External Network subnet (page 79).

Creating an External Network router

Cloud users can create routers to connect Private networks for their projects to the External Network subnet. Use this procedure to verify that a router can be connected.

Prerequisites

- Minimum required privileges: Cloud user
- An External Network subnet is created. See Creating the External Network subnet (page 78).
- The Private Network that you want to connect to the External Network subnet is configured and available for use.

Procedure 33 Creating a router to connect Private Network instances to the External Network subnet

1. If you are not already logged on to the CloudSystem Portal, log on.
2. From the **Project** menu, in the "Manage Network" section, select **Routers**.

   The **Routers** overview screen opens and displays a list of configured routers.
3. Select **+ Create Router**.

   The **Create router** screen opens.
4. Enter a name for the router, and then click **Create router**.

   Details about the new router are listed on the **Routers** overview screen.
5. Click **Set Gateway** next to the new router listing.
6. On the **Set Gateway** screen, select **External Network**, and then click **Set Gateway**.

   The **Routers** overview screen reopens.
7. Click the link for the new router to display its details screen.
8. Click **+ Add Interface**.
9. On the **Add Interface** screen, click the **Subnet** arrow and select the cloud network you want to connect to the External Network.
10. Click **Add interface**.

    The router details screen reopens and displays details about the new interface.

You can now use floating IP addresses to route traffic over the External Network subnet to specific virtual machine instances associated with a CloudSystem project. See Assigning floating IP addresses to instances (page 79).

Assigning floating IP addresses to instances

You can use floating IP addresses to route traffic over the External Network subnet to specific virtual machine instances associated with a CloudSystem project. Use this procedure to allocate and assign floating IP addresses.

Prerequisites

- Minimum required privileges: Cloud user
- An External Network subnet is created. See Creating the External Network subnet (page 78).
- A router is connected to the External Network subnet. See Creating a router to connect Private Network instances to the External Network subnet (page 79).
- The Private Network that you want to connect to the External Network subnet is configured and available for use.

Procedure 34 Assigning floating IP addresses to instances

1. If you are not already logged on to the CloudSystem Portal, log on.
2. Allocate IP addresses to a CloudSystem project.

a. From the **Project** menu, in the "Manage Network" section, select **Access & Security**.

   The **Security Groups** screen opens and displays configured security groups.

b. Select the **Floating IPs** tab.

c. Click **Allocate IP To Project**.

   The **Allocate Floating IP** screen opens and displays floating IP information for the project.

d. From the **Pool** list, select External Network, and then click **Allocate IP**.

   The **Allocate Floating IPs** screen reopens and displays the newly allocated floating IP addresses.

3. Associate a floating IP with an instance.

   a. From the **Project** menu, in the "Manage Network" section, select **Instances**.

   b. Next to the instance to which you want to assign a floating IP, click **More**, and then select **Associate Floating IP**.

      The **Manage Floating IP Associations** screen opens and displays floating IP information for the project.

   c. Click the **+** button under the **IP Address** field.

      The **Allocate Floating IP** screen opens.

   d. From the **Pool** list, select External Network, and then click **Allocate IP**.

      The **Manage Floating IP Associations** screen reappears with External Network listed in the **IP Address** field.

   e. Click **Associate**.

      The **Instances** screen reopens and displays the External Network floating IP address information associated with the instance.

4. Configure security group rules to enable SSH, ICMP, and other IP protocols on instances accessed using the External Network.

   a. From the **Project** menu, in the "Manage Compute" section, select **Access & Security**.

      The **Security Groups** screen opens and displays security groups configured for instances.

   b. Next to the security group associated with the instance, click **+ Edit Rules**.

      The **Security Group Rules** screen opens and displays all rules configured for the instance.

   c. Click **+ Add Rule**.

      The **Add Rule** screen opens.

   d. Select rules to define which traffic is allowed over the External Network to instances in the security group.

   e. Click **Add**.

      The **Security Group Rules** screen reappears and displays information about the added rule.

Users should now be able to access the instance using the associated floating IP from the External Network. To verify, use SSH on the External Network to reach the instance.

13 Integrated tool connectivity and configuration

CloudSystem Foundation enables the configuration of tools that expand its management capabilities. In this release, you can configure connectivity with a VMware vServer and a vServer proxy appliance, and with the HP Operations Orchestration Central software included with CloudSystem.

Managing integrated tools

CloudSystem Foundation Integrated Tools (page 81) lists each integrated tool, along with information about how to register and launch them.

Table 7 CloudSystem Foundation Integrated Tools

Integrated Tool	Used in CloudSystem to...	How to register	How to launch	URL
HP Operations Orchestration Central (page 81)	Attach workflows to server lifecycle actions or schedule flows for regular execution.	Registration is not needed.	Click the "HP OO Central" link on the **Integrated UIs** pane of the **Integrated Tools** screen.	https://*Foundation_IP*/OO
VMware vCenter Server (page 82)	Import ESX clusters.	Register VMware vCenter Server (page 82)	Enter the URL of the vCenter Server in a separate browser window.	https://*vCenter_Server_IP*

HP Operations Orchestration Central

OO Central contains a set of default workflows that allow you to manage administrative tasks associated with the private cloud.

OO Central is automatically installed as part of the CloudSystem Foundation appliance. CloudSystem Foundation supports full OO functionality, but only the workflows in the pre-defined bundle are available for use.

Installing OO Studio allows you to create new workflows to perform administrative tasks such as:

- Monitor provisioned virtual machines and send email notifications in the event of a failure.
- Check the status of memory, storage, and CPU usage.
- Run a health check on virtual machines.
- Apply patches to specific virtual machines.
- Schedule snapshot creation for specific virtual machines.

For information about installing OO Studio, see the *HP CloudSystem 8.0 Installation and Configuration Guide* at Enterprise Information Library.

For more information about HP Operations Orchestration, see http://www.hp.com/go/oo.

Using OO Central workflows

OO Central is automatically installed as part of CloudSystem Foundation. You can invoke general use workflows at any time. The workflows delivered with OO include:

- base-cp
- systems-cp
- virtualization-cp
- hp-solutions-cp
- cloud-cp

An executable file is also included in the tar file to support an installation of OO Studio. Installing OO Studio allows you to customize flows for general use cases. Customized flows can be saved as content packs and exported to a local directory. You can then pull those customized flows into OO Central. Workflows can be used to perform administrative tasks such as:

- monitor provisioned virtual machines and send email notifications in the event of a failure
- check the status of memory, storage and CPU usage
- run a health check on virtual machines
- apply patches to specific virtual machines
- schedule snapshot creation for specific virtual machines

Procedure 35 Working with OO workflows

Refer to the OO Studio documentation for more information on how to use OO Studio features. You can find documentation in the program folder you placed on your Windows system. Example: `C:/Program Files/Hewlett-Packard/HP Operations Orchestration/docs`

1. From the Windows system, log in to OO Studio
2. Load and test one of the flows imported into OO Studio.
3. Customize the flow and save it as a content pack.
4. Export the content pack to your local directory.
5. From the CloudSystem Console, select **Integrated Tools→OO Central**.
6. Log in with the OO Central user name and password. This is the same user name and password used to log in to the CloudSystem Console.
7. Import the saved flow from your local directory.
8. Select the **Library** tab.
9. Navigate to the imported flow and select it.
10. Click the **Run** button.

VMware vCenter Server

VMware vCenter Server is an appliance that is used to manage multiple ESX hosts through a single console application. VMware ESX is a virtualization platform on which you create and run virtual machines. vCenter Server acts as a central administrator for ESX hosts that are connected on a network. You can pool and manage the resources of multiple ESX hosts while monitoring and managing your physical and virtual infrastructure.

In CloudSystem, register vCenter Server as an integrated tool to establish a connection between the two appliances. Once vCenter Server is registered, ESX clusters can be imported from vCenter Server to the CloudSystem Console. The imported ESX clusters can then be activated and included in the cloud.

For more information, see VMware vSphere Documentation at VMware.

Register VMware vCenter Server

Use this procedure to register a connection to VMware vCenter Server in the CloudSystem Console. After the connection is made, you can import ESX clusters to be used as compute nodes.

Completing the configuration of the vCenter Server requires entering data on multiple screens and dialogs.

Prerequisites

- Minimum required privileges: Infrastructure Administrator
- A vCenter Server is installed and configured and connected to the network
- You have configured Cloud Networking settings. See Edit Cloud Networking (page 73).

Procedure 36 Registering vCenter Server

1. From the main menu, select **Integrated Tools**, then click **Register** in the VMware vCenter pane.
2. Enter data. Click "Help on this page" in the CloudSystem Console for more information.
3. Click **Register**.

   To exit the action without registering vCenter Server, click **Cancel**.
4. Verify that the updated number of registered vCenter Servers is displayed on the **Integrated Tools** screen.
5. Select **Edit vCenter Server IP list** from the **Actions** menu, or click the “not set” link next to **IPs for vCenter proxy appliance**.

   Each vCenter proxy appliance requires an IP address on the Data Center Management Network. This address can be obtained from DHCP or statically. If static IP addresses are preferred, plan to provide 1 static IP address for each vCenter proxy appliance, for every 12 clusters.
6. Enter data.

   If static IP addresses are used, enter unused addresses from the Data Center Management Network so that they can be assigned to the proxies as they are deployed.

   Click "Help on this page" in the CloudSystem Console for more information.
7. Click **Save**.

   To exit the action without saving the IP address type, click **Cancel**.
8. Verify that the vCenter proxy appliance link displays the IP address type, instead of the “not set” link.
9. Find the line for **Datacenter switch definitions** and click the “not set” link.
10. Enter data. Click "Help on this page" in the CloudSystem Console for more information.
11. Click **Save**.

    To exit the action without saving the switch definition, click **Cancel**.
12. Verify that the Datacenter switch definition link displays the **configured** link.

14 Image management

Use the information in this chapter to learn how to bring existing images into CloudSystem Foundation for use in provisioning virtual machines. From CloudSystem Console, you can create new images from virtual machines running in the cloud.

This chapter does not cover creating an image from scratch. To learn how, see documentation available on the Enterprise Information Library or at OpenStack Software.

About Images

An image contains the operating system for a virtual machine. It defines the file system layout, the OS version, and other related information about the operating system to provision. An image can be provisioned to one or more virtual machines in the cloud.

Images in the cloud

Images that you add (upload) are used to boot virtual machine instances in the cloud.

Before virtual machine instances can be provisioned in the cloud, you must create at least one provider or private network, and upload at least one image. Using the CloudSystem Console, you upload images by doing one of the following:

- Entering a file server URL
- Selecting a local file
- Creating an image from a snapshot of a currently running instance. See Create image from a snapshot of a virtual machine (page 86).

Managing images

From the **Images** overview screen on the CloudSystem Console, you can view data about existing images, including how many virtual machine instances are running a particular image. You can also access the **Add Image** screen to upload one or more images.

After you upload an image using the console, cloud users can then use the CloudSystem Portal to choose from available images, or create their own from existing servers. Users can also create images using OpenStack API or CLI.

As Infrastructure administrator, you can use either the console or the service portal to edit and delete images.

Image format support

- **ESX**: *Flat* and *Sparse* Virtual Machine Disk format (VMDK) image files with SCSI adapters are supported for VM guest provisioning on VMware ESX hypervisors. Other formats including compressed VMDK images, and IDE adapters, are not supported.

  If your image uses the Sparse VMDK format, you must set the required properties on the image using the OpenStack Glance CLI.

  See the *OpenStack Configuration Reference* at OpenStack Cloud Software for information about configuring VMware-based images for launching as virtual machines.

- **KVM**: Quick EMUlator (QEMU) copy-on-write format (QCOW2) formatted image files are supported for virtual machine provisioning on KVM hypervisors. Other formats are not supported.

Image naming and single datastore support in VMware vCenter Server

- Each set of CloudSystem images must be in the same datastore in the vCenter Server.
- Folders cannot be used to separate an additional set of CloudSystem images that are uploaded to the vCenter Server.
- For example, if the Enterprise appliance image is added after the Foundation image, the Enterprise image must be uploaded to the same datastore as the running Foundation appliance, and it must have a unique name from other Enterprise appliances running in the same vCenter Server.

Image metadata

Openstack Compute (Nova) uses a special metadata service to allow instances to retrieve specific instance data. CloudSystem supports the OpenStack metadata API. The Amazon Elastic Compute Cloud (EC2)–compatible API is not supported.

Can I delete images after they are provisioned?

Yes. Since images are downloaded to the virtual machine instances running the images, you can delete images after they are provisioned without affecting the instances. Deleting an image removes it from the console and user portal, making it unavailable for use when deploying virtual machine instances.

Before you delete an image, you must check the **Read-only** setting for the image and, if necessary, set it to **Disabled**. You can change this field on the Edit Image screen.

Deleting an image changes its screen components.

- In the CloudSystem Console, the **Image** value for each previously associated instance changes to **Missing**. To check this value, select **Instances** from the main menu.
- In the CloudSystem Portal, the **Status** value for the image changes to **Deleted**.

To make a deleted image available for use again, use the **Add Image** screen in the console. See Add Image (page 86).

Creating and obtaining images

For information about creating and obtaining images that you can add to the CloudSystem Console, see the *OpenStack Virtual Machine Image Guide* at *OpenStack Cloud Software*.

Setting custom attributes on Microsoft Windows images

Before you can use a Windows image (.VMDK file) to boot ESX virtual machines, you must set custom attributes on the image using the OpenStack Glance CLI or API. (Setting attributes is not required for Linux images on ESX or KVM.)

The custom attributes required for Windows images on ESX are (for example):

- `vmware_ostype=windows8Server64Guest` *This line shows one possible example of a Windows operating system type*
- `vmware_adaptertype=lsiLogicsas`

Set the custom attributes in one of the following ways.

After uploading a Windows image using the Add image screen

After you upload a Windows image using the **Add Image** screen, use the Glance CLI to set the attributes on the file.

On a Windows or Linux system where the OpenStack CLI package for CloudSystem is installed, enter the following command, where *Windows-image.vmdk* is the name of your Windows image to update:

```
glance --insecure image-update --name <Windows-image.vmdk> --property vmware_ostype=windows8Server64Guest
--property vmware_adaptertype=lsiLogicsas
```

While uploading a Windows image using the Glance CLI

When you use the OpenStack Glance CLI to upload the image, you can set the attributes and upload the image at the same time.

On a Windows or Linux system where you installed the OpenStack CLI package for CloudSystem and which contains the image to upload, enter the following command, where *Windows-image.vmdk* is the name of the Windows image, and *new-Windows-image.vmdk* is the name of the modified image that is uploaded to CloudSystem:

```
glance --insecure image-create --name <Windows-image.vmdk> --disk-format=vmdk --container-format=bare --file
<new-Windows-image>.vmdk --property vmware_ostype=windows8Server64Guest --property vmware_adaptertype=lsiLogicsas
```

For information about installing the OpenStack CLI packages for CloudSystem on a Windows or Linux system see the *HP CloudSystem Installation and Configuration Guide* at Enterprise Information Library. These packages allow you to run the supported OpenStack Nova, Glance, Keystone, Neutron, and Cinder commands.

For more information, see OpenStack glance commands at OpenStack Cloud Software.

Create image from a snapshot of a virtual machine

Use this procedure to create an image from a snapshot of a currently defined virtual machine instance. You can also accomplish this action in the CloudSystem Portal. By creating an image from a known instance, you can copy the attributes of the instance into the format of an image, so that you can use it to create other instances.

You can create an image of an instance from a running instance or from an instance that is paused. If the instance is running at the time of the snapshot, the instance is paused before the snapshot is taken. The instance is automatically restarted after the snapshot is captured.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The state of the instance is **Active** or **Paused**.

Procedure 37 Creating an image from a snapshot of an instance

1. From the main menu, select **Instances**.

   The **Instances** overview screen is displayed.
2. Select the instance from which you want to create the new image.
3. Select **Actions→Create image**.

   The **Create image from a snapshot server instance** screen is displayed.
4. Enter the following information:
   - The name of the image to be created.
   - A description (optional).
5. To complete the action, click **Create**.
6. Verify that the image is displayed on the Images overview screen.

Add Image

Use this procedure to add an image that can be used to create an instance.

For information about creating an image from a server instance, see Create image from a snapshot of a virtual machine (page 86).

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The image to upload is contained in a single file. You cannot upload a multipart disk image (for example, a kernel image and a RAM disk image).
- If you use the **Select local file** option, the size of image file to upload is not more than:
  - 4 GB if your browser is Microsoft Internet Explorer or Mozilla Firefox
  - 20 GB if your browser is Google Chrome

Procedure 38 Adding Images

1. From the main menu, select **Images**.
2. Click **Actions→Add**.
3. Select one of the following:
   - **Enter file URL**. Enter the URL (beginning with http:) of the image to upload from a file server accessible to the host management subnet. For example, `http://fileserver.com:port/dir1/imagename`.
   - **Select local file** to display a file selection dialog. Select a single file that contains the image.
4. Enter data for this image. Select "Help on this page" in the CloudSystem Console for more information.

   A search field is provided for locating a previously defined description for use in the Description field. Begin typing to start the search. If no matching entries are found, click the magnifying glass to the right of the field. A **Search for another** link will appear in the drop-down list. Clicking this link displays all saved descriptions.
5. To finish adding the image, click **Add**.

   To exit without uploading an image, click **Cancel**.
6. Verify that the image was added on the **Images** overview screen.

   See also Troubleshooting images (page 162).
7. Set custom attributes on Windows images using the OpenStack Glance CLI.

   See Setting custom attributes on Microsoft Windows images (page 85).

Procedure 39 Adding multiple images in one action

1. From the main menu, select **Images**.
2. Click **Actions→Add**.
3. Enter data for this image.
4. Click **Add +** to complete this image and reset the form for entering another new image.
5. Repeat steps 3 and 4 until you are finished adding multiple new images, then click **Cancel** to dismiss the **Add** screen.
6. Verify that the images were added on the **Images** overview screen.

Edit Image

NOTE: From the Edit image screen, you can change only the metadata of images.

Use the **Edit Image** screen to edit the image name and description, change the OS type, disk format, and container format, and change the value of the Shared and Read-only settings.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 40 Editing Images

1. From the main menu, select **Images**.
2. Select the row of the image to be edited.
3. Click **Actions→Edit**.
4. Update the image information. Select "Help on this page" in the CloudSystem Console for more information.

   A search field is provided for locating a previously defined description for use in the Description field. Begin typing to start the search. If no matching entries are found, click the magnifying glass to the right of the field. A **Search for another** link will appear in the drop-down list. Clicking this link displays all saved descriptions.
5. To apply the changes to the image metadata, click **OK**.

   To exit without making changes, click **Cancel**.
6. Verify that the image metadata is correct on the **Images** overview screen.

Delete Image

Use this procedure to remove an image from the CloudSystem Console and the CloudSystem Portal, making it unavailable for use when deploying virtual machine instances.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The **Read-only** option is set to **Disabled** for the image.

Procedure 41 Deleting Images

1. From the main menu, select **Images**.
2. Select the row of the image to be removed.
3. Click **Actions→Delete**.
4. Click **Yes, delete** to complete the deletion.

   To exit without making changes, click **Cancel**.
5. With the filter set to **All OS types**, verify that the image was deleted from the **Images** overview screen.

15 Storage configuration

CloudSystem Console provides the capability to manage and track the use of block storage drivers, volumes and volume types.

Managing Storage

Block storage drivers deliver the technology or vendor-specific implementations for the OpenStack Block Storage (Cinder) functionality. CloudSystem Foundation supports direct attached storage for 3PAR Fibre Channel and iSCSI drivers. These drivers are connected to the management console of supported HP 3PAR storage systems.

Volume types are associated with block storage drivers. When creating volume types, the type of driver along with other specified storage parameters help define the provisioning characteristics of the storage volumes. This provides a template that the cloud users can use to create volumes.

A block storage driver and a volume type must be defined before creating a volumes in the CloudSystem Portal. The CloudSystem Console provides the ability to view the statuses of the volumes and to delete volumes that are detached from VM instances.

Managing block storage drivers

Authorized infrastructure administrators use the CloudSystem Console to manage block storage drivers. Adding these drivers is the first step in configuring your storage solution. Before you can add a volume type or a volume, you first must have a driver to associate with the volume type.

You can add multiple driver types (Fibre Channel or iSCSI) to a storage system. When adding one FC driver type and one iSCSI driver type to the same storage system, both must reside in the same domain. Also, when adding an iSCSI driver you must have connectivity from the targeted compute node to the 3PAR storage system iSCSI port. If you do not configure the connection, block storage volumes will not attach to virtual machine instances.

After you have added the block storage drivers, you can use the CloudSystem Console to edit them or delete them from the storage system. You only can delete block storage drivers that are *not* associated with a volume type. If a block storage driver is associated with a volume type, you must first delete the volume type before you can delete the driver.

Understanding block storage drivers data

The driver name and type (Fibre Channel or iSCSI) are shown in the **General** section.

The number of volume types and volumes to which each driver is associated, and the storage area network (SAN) data transfer standard (Fibre Channel or iSCSI) used by the volume type are displayed in the **Details** section.

The capacity (in terabytes) of each driver is displayed in the **Utilization** section. The capacity is displayed as the amount being used in relationship to the total available capacity. For example, 23.2 of 25 TB.

Block storage driver data is displayed on the Block Storage Driver overview screen. The displayed data providess details for each of the drivers you added, including the driver name and type, volume type and volume association, and the capacity of each driver.

Add Block Storage Drivers

Use this procedure to add a block storage driver for management in the CloudSystem

Prerequisites

- Minimum required privileges: Infrastructure administrator
- You must have connectivity from the targeted compute node to the 3PAR storage system iSCSI port when adding an iSCSI driver. If you do not configure the connection, block storage volumes will not attach to virtual machine instances.

Procedure 42 Adding a block storage driver

1. From the main menu, select **Block Storage Drivers**.

   The **Block Storage Drivers** overview screen is displayed.
2. Click **+ Add Block Storage Driver**.

   The **Add Block Storage Driver** screen is displayed.
3. Enter the required information . Click "Help on this page" in the CloudSystem Console for details.
4. Do one of the following:
   - To add only this block storage driver, click **Add**. The block storage driver is displayed on the overview screen.
   - To add more than one block storage driver:

   a. Click **Add+** to complete the first addition and reset the form. The fields are cleared for reuse.

   b. Enter a unique name for the block storage driver.

   c. Update additional field values, if needed.

   d. Repeat steps a, b, and c until you are finished adding additional block storage drivers, then click **Cancel** to dismiss the **Add** screen. Clicking **Cancel** displays the overview screen with the new block storage drivers.
5. Verify that each new block storage driver is displayed on the **Block Storage Driver** overview screen. Click the **Name** column heading to sort the block storage drivers by name.

Edit Block Storage Drivers

Use this procedure to edit block storage driver attributes.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- You must have connectivity from the targeted compute node to the 3PAR storage system iSCSI port when editing an iSCSI driver. If you do not configure the connection, block storage volumes will not attach to virtual machine instances.

Procedure 43 Editing a block storage driver

1. From the main menu, select **Block Storage Drivers**.

   The **Block Storage Drivers** overview screen is displayed.
2. Select **Actions→Edit**.

   The **Edit Block Storage Driver** screen is displayed.
3. Enter the required information . Click "Help on this page" in the CloudSystem Console for details.
4. To save the changes, click **OK**.
5. Verify that the changes are displayed on the **Block Storage Driver** overview screen. Click the **Name** column heading to sort the block storage drivers by name.

Delete Block Storage Drivers

Use this procedure to delete block storage drivers.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The block storage driver is not assigned to a volume type. See Delete Volume Types (page 93).

Procedure 44 Deleting Block Storage Drivers

1. From the main menu, select **Block Storage Drivers**.
2. Select the block storage driver you want to delete.

   NOTE: If the block storage driver is assigned to a volume type it cannot be deleted. You must delete the associated volume type before deleting the driver. See Delete Volume Types (page 93).

3. Select **Actions** →**Delete**.
4. To confirm and delete the driver, click **Yes, delete**.

   To exit the action without deleting the driver, click **Cancel**.
5. With the filter set to **All statuses**, verify that the driver no longer appears on the **Block Storage Drivers** overview screen.

About volume types

Authorized infrastructure administrators use the CloudSystem Console to configure and manage volume types. When configuring storage systems, the volume types define specific storage characteristics.

How are volume types used?

When you configure your storage systems, you must attach a block storage driver to each volume type. The volume types, in turn, help define the characteristics of the volumes that are created by the cloud users.

Managing volume types

Before adding a volume type, the following storage conditions must exist:

- 3PAR F-Class, P7000 or P10000 storage system is installed in the environment.
- Sufficient space is available on the 3PAR storage system.
- HP 3PAR OS 3.1.2 MU2 is installed.
- IMC V4.4.0 is installed.
- Fibre Channel fabric support.
- REST API interface must be enabled on the 3PAR.
- One domain with one CPG is required.
- At least one block storage driver has been added.

Volume types added using the CloudSystem Console can be edited in the CloudSystem Console. If you created a volume type outside of the console; for example, using the OpenStack Nova or Cinder CLI, you cannot edit the volume type in the console.

Understanding volume types data

Volume types data provides details for each of the volume types you add.

The maximum input/output per second is the number of 4K or 8K blocks of data per second that can be sent to a disk when accessing databases or other online access. The maximum blocks in megabytes (MB) per second is the throughput determined for each volume type. For example, 300 MB/s can sustain large I/O blocks (64K or greater) of data at that rate when performing sequential access during backups or video streaming. The number of Fibre Channel (FC) ports, and the number of iSCSI ports that are available for use are also displayed.

See the **Volume Types** overview screen for other useful information .

What is the benefit of thin provisioning?

When configuring virtual capacity, thinly-provisioned volume types better maximize the use of your storage than those that are fully-provisioned. Thinly-provisioned volume types reserve the storage space you specify, and use only what is needed. Any unused storage capacity is then allocated to satisfy requirements in other areas. Fully provisioned volume types reserve the full allocated amount of storage space whether used or not, and are not able to take advantage of reallocating any available unused capacity.

Thin provisioning provides the benefit of not having to allocate more storage and being able to scale your system without needing to purchase additional hardware.

Add Volume Types

Use this procedure to add volume types. After a volume type is added, you can manage it from the overview screen.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- At least one block storage driver has been added

Procedure 45 Adding volume types

1. From the main menu, navigate to **Volume Types**.
2. Click **+ Add Volume Type**.
3. Enter the data. Select "Help on this page" in the CloudSystem Console for more information.

   NOTE: When you add a volume type to be used for volumes that will be attached to ESX virtual machine instances, you must select the correct host mode.

   Select **VMware** for ESX compute volume types and **Generic** for KVM compute volume types.

4. Do one of the following:
   - To add only this volume type click **Add**. The volume type is displayed on the overview screen.
   - To add more than one volume type:
   a. Click **Add+** to complete the first volume type addition and reset the form. The **Name** field is cleared, but all other field values will display for reuse.
   b. Enter a unique name for the volume type.
   c. Update other field values, if needed.
   d. Repeat steps a, b, and c until you are finished adding additional volume types, then click **Cancel** to dismiss the **Add** screen. Clicking **Cancel** displays the new volume types on the overview screen.
5. Verify that each new volume type is displayed on the **Volume Types** overview screen. Click the **Name** column heading to sort the volume types by name.

Edit Volume Types

Use this procedure to edit volume types. After the volume type is edited, you can manage it from the overview screen.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 46 Editing volume types

1. From the main menu, click **Volume Types**.
2. Click **Actions**→ **Edit**.
3. Edit the data. Select "Help on this page" in the CloudSystem Console for more information.
4. To save the changes, click **Save**.

   To exit the action without making changes, click **Cancel**.
5. Verify that each new volume type is displayed on the **Volume Types** overview screen.

Delete Volume Types

Use this procedure to delete Volume Types. After a volume type is deleted, it is removed from the overview screen.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 47 Deleting volume types

1. From the main menu, click **Volume Types**.
2. Select the volume type you want to delete.
3. Click **Actions** →**Delete**.
4. To confirm and delete volume type, click **Yes, delete**.

   To exit the action without deleting the volume type, click **Cancel**.
5. With the filters set to **All statuses** and **All driver types**, verify that the volume type no longer appears on the **Volume Types** overview screen.

About Volumes

Volumes provide persistent block storage for virtual machine instances. OpenStack technology provides two classes of block storage: ephemeral storage and persistent volumes. *Ephemeral* storage is assigned to a VM instance when the instance is created and then released when the instance is deleted. All instances have some ephemeral storage.

When you create a VM instance, you select a predefined flavor. The definition of a flavor includes the number of virtual CPUs, the amount of random access memory (RAM), and the amount of disk space allocated for storage. Storage defined as part of the flavor definition is ephemeral.

Block storage volumes (also known as OpenStack Cinder volumes) persist as independent entities. A block storage volume can exist outside the scope of a VM instance. Once created, a block storage volume can be attached to one VM instance and later can be detached. The detached block storage volume can then be attached to a different VM instance.

Managing Volumes

You perform most volume management tasks through the CloudSystem Portal or OpenStack API and CLI (see Provision a cloud in Foundation (page 117) for more information). From the CloudSystem Portal, you can create and delete volumes, and attach volumes to or detach volumes from VM instances.

In addition to the details displayed on the Volumes overview screen, you can find other data in the Volumes area of the CloudSystem Portal.

Before you can create a volume in the CloudSystem Portal, you must use the CloudSystem Console to create a block storage driver and associate it with a volume type.

From the CloudSystem Console, you can monitor the status of the volumes and delete volumes not attached to a VM instance. See Delete Volumes (page 95) for more information.

Understanding Volumes data

Volumes data is displayed on the **Volumes** overview screen. The displayed data provides details for each storage volume that is created in the CloudSystem Portal.

The displayed data includes the volume name, size (in gigabytes), status (such as Creating, Deleting, Available, In-use, and Error), associated volume type, and if attached to a VM instance, the name VM instance to which it is attached.

NOTE: Volumes created in the CloudSystem Portal have prefixes of OSV (OpenStack Volume) or OSS (OpenStack Snapshot).

Create volumes in the CloudSystem Portal

The **Volumes** overview screen in the CloudSystem Console displays data after you create block storage volumes in the CloudSystem Portal. Block storage drivers and volume types are used to define the characteristics of the block storage volumes to which they are associated.

Use the following procedure to create a volume.

Prerequisites

- Minimum required privileges: Cloud user
- You must have added a volume type and associated it with a block storage driver using the CloudSystem Console. See Add Volume Types (page 92).
- You must be logged on to the CloudSystem Portal.

NOTE: The portal is accessed by appending /portal to the Foundation appliance URL (for example, `https://192.0.2.2/portal`).

Procedure 48 Creating volumes in the CloudSystem Portal

NOTE: Be sure to select a volume type when creating a volume. The volume type is necessary to ensure that the volume attaches correctly to a VM. Also ensure that you use a unique name for each volume. Volume names must be unique, since they are used with different targets.

---

1. From the **Project** tab, select **Manage Compute**→ **Volumes**.

   The **Volumes** screen is displayed.
2. Click the **+Create Volume** button.

   The **Create Volume** screen is displayed.
3. Complete the required fields, and click the **Create Volume** button to complete the action. Clicking **Cancel** returns to the **Volumes** screen without completing the action.
4. Verify that the volume you created is displayed on the **Volumes** screens in the CloudSystem Portal and the CloudSystem Console.

Attach a volume to a VM instance in the CloudSystem Portal

Volume attachments are managed in the CloudSystem Portal.

Use the following procedure to attach a volume to a VM instance.

Prerequisites

- Minimum required privileges: Cloud user
- You must have created at least one volume with an associated volume type. See Create volumes in the CloudSystem Portal (page 94).
- You must be logged on to the CloudSystem Portal.

NOTE: The portal is accessed by appending /portal to the Foundation appliance URL (for example, `https://192.0.2.2/portal`).

Procedure 49 Attaching volumes in the CloudSystem Portal

1. From the **Project** tab, select **Manage Compute→Volumes**.

   The **Volumes** screen is displayed.
2. Click the check box next to the name of the volume you want to attach.
3. In the **Action** column, click **Edit Attachments**

   The **Manage Volume Attachments** screen is displayed.
4. In the **Attach To Instance** drop-down, select the VM instance to which you want to attach the volume.
5. Edit the **Device Name** if necessary.
6. Click **Attach Volume** to complete the action. Clicking **Cancel** returns to the **Volumes** screen without completing the action.
7. Verify that the volume you attached is displayed in the **Attached To** columns on the **Volumes** screens in the CloudSystem Portal and the CloudSystem Console.

   NOTE: If the volume cannot be attached to the device you specified (for example `/dev/vdc` is specified), the device is ignored and the guest operating system automatically attaches the volume to the next available device (for example `/dev/sdc` is where the volume attached).

Delete Volumes

Prerequisites

- Minimum required privileges: Infrastructure administrator
- Volumes must be detached from their associated VMs.

Procedure 50 Deleting Volumes

1. From the main menu, click **Volumes**.
2. Select the volume to delete.
3. Select **Actions →Delete**.
4. To confirm and delete the volume, click **Yes, delete**.

   To exit without deleting the volume, click **Cancel**.
5. With the filters set to **All statuses**, verify that the volume does not appear on the **Volumes** overview screen.

16 Compute node creation

Compute nodes manage the resources required to run instances in the cloud. In CloudSystem, two types of compute nodes are supported: ESX and KVM.

- You create and manage **ESX** compute hosts in vCenter Server. All compute hosts are configured as clusters and must be imported into CloudSystem. After import, you can activate clusters and create instances that consume the resources.
- You create **KVM** compute nodes on KVM hosts. After a compute node is created, the Data Center Management Network allows CloudSystem to see the compute node. The compute node displays on the Compute Nodes overview screen in an Unknown status, meaning it is not yet activated. After activating the compute node, you can create instances that consume the resources.

Preparing compute nodes

To determine the size of your compute node, answer the following questions.

- What flavor settings will the provisioned instances use? See About Flavors (page 109).
- What oversubscription rate is supported for each compute resource? See Calculating the number of instances that can be provisioned to a compute node (page 105).
- How many instances will each compute node support?

After answering the questions above, determine the amount of CPU cores, memory and storage to allocate to each compute node. You might want to consider Maximum supported configuration values for each CloudSystem (page 71).

Creating ESX compute hypervisors

ESX compute hosts are created inside clusters in vCenter Server. Consult VMware documentation for instructions on creating and configuring compute hosts in vCenter Server.

See VMware vSphere Documentation at VMware for all details on using and configuring vSphere software.

Preparing or completing each of the following requirements can help to ensure success in creating a correctly configured ESX cluster for import into CloudSystem.

Table 8 ESX compute host checklist

☑	Requirement	Additional Resources
	You have administrator privileges to log in to VMware vCenter Server	VMware vSphere Documentation
	A management hypervisor is fully configured in a cluster in vCenter Server and the base appliance, SDN appliance, and network node appliances are created. You can create some compute hosts in the management vCenter Server, but HP recommends creating them in a separate compute vCenter Server.	*HP CloudSystem 8.0 Installation and Configuration Guide* at Enterprise Information Library.
	A compute Datacenter is set up and contains a cluster and compute hosts. DRS is enabled.	VMware vSphere Documentation
	Supported software for the host is ESXi 5.0.3, 5.1.2 and 5.5 (Custom HP image)	VMware vSphere Documentation
	The host name for each compute host in the cluster has a matching host name in any connected 3PAR storage system.	--

Table 8 ESX compute host checklist *(continued)*

☑	Requirement	Additional Resources
	The host name must be specified as a FQDN and not an IP address.	
	You have a standard or distributed vSwitch on the Cloud Data Trunk for each cluster. See Configuring networks (page 97)	VMware vSphere Documentation
	A large datastore supports all hosts in the cluster. The datastore must be in the same Datacenter where the vSwitch is configured.	VMware vSphere Documentation
	To use the security groups feature, VMware vShield Manager in vCNS must be installed and configured for the managed vCenter Server. vShield App must be installed from vShield Manager on each host in the management vCenter Server cluster. Configuring security groups for instances in an ESX cluster (page 98)	*vSphere Virtual Machine Administration Guide*
	Optional: For console access in the CloudSystem Portal, the port range 5900 to 6105 is open for each compute host.	OpenStack Documention for Havana releases
	Optional: If you plan to connect to 3PAR using iSCSI, then you have connectivity to the iSCSI network that is connected to the 3PAR. Configuring iSCSI on ESX compute hosts (page 98)	*HP CloudSystem 8.0 Installation and Configuration Guide* at Enterprise Information Library

Configuring networks

A virtual switch (distributed or standard) is configured on the Cloud Data Trunk to support all compute hosts in the compute cluster. The number of VLAN IDs assigned to the Cloud Data Trunk is the number of Provider and Private networks you can create in CloudSystem.

Distributed virtual switches

A distributed vSwitch supports all hosts in a compute cluster, and all hosts in the compute clusters within the same data center must be connected to the same distributed vSwitch. The distributed vSwitch also should be attached to the virtual machine NICs of all the compute hosts. For ESX clusters, you can use the default vSphere Distributed Switch (vDS) when creating the vSwitch. If you have more than one host in the cluster, ensure that **vmotion** is configured on the Data Center Management Network.

Standard virtual switches

When standard vSwitches are used, one vSwitch is configured for each compute host. The vSwitch name must be the same for each host. The vSwitch name is defined when you register the vCenter Server on the **Integrated Tools** screen of the CloudSystem Console.

Configuring security groups for instances in an ESX cluster

Security group functionality is provided by VMware vCNS, and not by the security group rules configurable from the CloudSystem Portal. To enable the security groups feature in an ESX environment, the following must be true.

- VMware vShield Manager virtual appliance must be installed and configured for each managed vCenter Server, as a single vShield Manager can serve only a single vCenter Server environment.
- vShield App virtual appliance must be intalled from vShield Manager on each ESX host in the cluster that is managed from the managed vCenter Server.
- CloudSystem Foundation requires that all vShield Manager certificate names match compute host names.

To learn how to configure security groups using vShield Manager and vShield App, refer to the *vShield Administration Guide* at VMware.

Configuring iSCSI on ESX compute hosts

If you plan to attach iSCSI volumes created in the HP 3PAR storage system to instances hosted on VMware ESX servers, then you must configure an iSCSI adapter on the ESX compute hosts.

Configuring networking for the VMkernel

A single VMkernel adapter is required to support iSCSI. The VMkernel runs services for iSCSI storage and must be connected to a physical network adapter.

Prerequisites

- SAN storage hardware is using HP 3PAR firmware version 3.1.2

Procedure 51 Configuring networking for the VMkernel

1. Log in to the vSphere Client hosting your vCenter Server and select a compute host from the **Inventory** panel.
2. Select the **Configuration**→**Networking** tab.
3. From the vSphere Standard Switch view, select **Add Networking**.
4. Select **VMkernel** and click **Next**.
5. To create a new standard switch, select **Create a vSphere standard switch**.
6. Select the NIC to use for iSCSI traffic and click **Next**.
7. Enter a network label and click **Next**.

   The label helps you easily identify the VMkernel adapter.
8. Specify the IP settings and click **Next**.
9. Review the information and click **Finish**.

After configuring the VMkernel networking, you need to bind the iSCSI adapter with the VMkernel adapter. You can find a list of available storage adapters in the **Hardware** tab under **Storage Adapters**. When the VMkernel adapter is bound with the iSCSI adapter, you see a network connection on the list of VMkernel port bindings for the iSCSI adapter.

Setting the discovery address and target name of the storage system

The iSCSI adapter uses the target discovery address to determine which storage resources on the network are available for access.

Dynamic discovery

When using dynamic discovery, a SendTagets request is sent to the iSCSI server every time the initiator contacts the server. To use this type of discovery, you must associate your storage adapter with an iSCSI initiator, and set that initiator to use dynamic discovery. Each time the host sends out the request for targets, the Static Discovery list is populated with newly discovered targets.

Static discovery

With static discovery, iSCSI target information is added manually. To use this type of discovery, you must associate your storage adapter with an iSCSI initiator and set that initiator to use static discovery.

Next steps:

- Register VMware vCenter Server (page 82)
- Import a cluster (page 105)
- Activate a compute node (page 105)

Creating KVM compute nodes

KVM compute nodes are created on hypervisor hosts. Consult *Red Hat Enterprise Linux 6 documents* for instructions on creating and configuring KVM compute nodes.

Preparing or completing each of the following requirements can help to ensure success in creating a correctly configured KVM compute node.

Table 9 KVM compute node checklist

☑	Requirement	Additional Resources
	RHEL 6.4 is installed on the compute hypervisor.	*Red Hat Enterprise Linux 6 documents*
	If you are using the RHEL default driver, **Broadcom TG3 NIC**, then you must update the driver.	HP Support Center
	If you are using the Emulex driver, **be2net**, then you must upgrade to version 4.4.245.0 or later.	Citrix support
	You have allocated adequate disk space for a `/var/lib/nova/instances` directory that can support all anticipated provisioned instances.	--
	The host name for each compute host in the cluster has a matching host name in any connected 3PAR storage system. The host name must be specified as a FQDN and not an IP address.	--
	Optional: For console access in the CloudSystem Enterprise, the port range 5900 to 6105 is open for each ESX compute node.	OpenStack Documention for Havana releases
	Optional: If you plan to connect to 3PAR using iSCSI, then you have connectivity to the iSCSI network that is connected to the 3PAR.	*HP CloudSystem 8.0 Installation and Configuration Guide* at Enterprise Information Library

Applying CloudSystem requirements to the KVM compute node

After the compute node is created and the operating system is installed, you can complete the specific CloudSystem requirements. The procedures in this section explain how to prepare your KVM compute node for use in the cloud.

Creating a local YUM repository and validating dependencies

An RHEL KVM dependencies package is included in the CloudSystem Tools `.zip` file that you download from HP Software Depot. This package is an empty RPM that lists required RHEL dependencies.

Once a YUM repository is created, you can run the dependencies package. The repository must point to the RHEL ISO or YUM repository where the RPMs are stored, to allow the package to scan the list. After the package is run on the compute node, a list of missing dependencies is displayed for troubleshooting.

If you are missing dependencies, download them and then place them in your local YUM repository.

Table 10 Required RHEL dependencies

avahi	MySQL-python	python-paramiko
bridge-utils	netcf >= 0.1.9-3	python-paste
bind-utils	net-tools	python-qpid
compat-openldap	ntp	python-tempita
fuse	openssh-clients	python-twisted-core
gawk	openssl098e	python-twisted-web
grep	PyPAM	rsync
GConf2	python-cheetah	scsi-target-utils
gstreamer-plugins-base	python-decorator	sed
kpartx	python-ldap	sgml-common
libguestfs-mount	python-libguestfs	tunctl
libguestfs-tools	python-lxml	unixODBC
libtool-ltdl	python-mako	vconfig
libvirt	python-memcached	xorg-x11-drv-cirrus
libvirt-python >=0.9.10	python-netaddr	xorg-x11-drv-fbdev

Prerequisites

- **rhel-kvm-deps-8.0.0.xx rpm** is extracted from the **CloudSystem-Tools-8.0.0.xx.zip** file and moved to a Linux system.

Procedure 52 Creating a local YUM repository and validating dependencies

You can use a utility such as WinSCP (http://winscp.org/), to create the YUM repository and validate dependencies.

1. Make a new directory and copy RHEL 6.4 to a directory location such as `/home/kits`:
   ```
   # mkdir /home/kits
   ```
2. Make a new directory for the DVD mount point:
   ```
   # mkdir /dvd
   ```
3. Mount the DVD:
   ```
   # mount –o loop /home/kits/rhel-server-6.4-x86_64-dvd.iso /dvd
   ```
4. Create the repository:
   a. `# cd /etc/yum.repos.d/`
   b.
   ```
   # vi LocalDCRhel.repo
   [RHELDVD]
   name=Locally Mounted RHEL 6.4 ISO
   baseurl=file:///dvd/
   enabled=0
   ```
5. Import the GPG-Key (GNU Privacy Guard):
   a. `# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release`
   b. `# yum clean all`
   c. `# yum update`
6. Install the dependency packages:
   ```
   yum install –y rhel-kvm-deps-8.0.0.xx.rpm --enablerepo=RHELDVD
   ```
   Missing dependencies are identified and installed.

7. Verify that the **libguestfs** and **libguestfs-tools** packages were installed:

```
yum list | grep libguestfs*
```

Configuring CloudSystem compute node network settings

Prerequisites

- RHEL 6.4 is installed on the compute node.
- Dependency packages are installed on the compute node. See Creating a local YUM repository and validating dependencies (page 99)
- Checklist of requirements is completed for the compute node.

Procedure 53 Configuring CloudSystem compute settings

1. Log in to the compute node.
2. Configure the network device where the Cloud Management Network is plumbed.

   In the example below, **ethM** represents the network device:

```
DEVICE="ethM"
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
PEERDNS="no"
PERSISTENT_DHCLIENT=1
DHCP_HOSTNAME=<short_hostname_of_your_compute_node>
```

   The DHCP_HOSTNAME should be the short host name of the compute node. On the Foundation base appliance, the DHCP server uses this value to determine the base host name to prepend to the `hpiscmgmt.local` domain to get the fully-qualified domain name for the base appliance.
3. Bring up the Cloud Management Network:

```
ifdown ethM
ifup ethM
```

4. Configure the network device where the Data Center Management Network is plumbed.

   In the example below, **ethN** represents the network device.

```
DEVICE=ethN
...
IPADDR=<your management network IP address>
NETMASK=<your management network NETMASK>
NM_CONTROLLED="no"
PEERDNS="no"
PERSISTENT_DHCLIENT=1
BOOTPROTO="static"
ONBOOT="yes"
...
```

   Save the change and close the file.
5. Bring up the Data Center Management Network:

```
ifdown ethN
ifup ethN
```

6. Configure the network device where the Cloud Data Trunk is plumbed.

   In the example below, **ethP** and **ethQ** represent the network device.

```
DEVICE=[eth-P] or [eth-Q]
...
NM_CONTROLLED="no"
PEERDNS="no"
ONBOOT="yes"
```

```
BOOTPROTO="none"
...
```

Save the change and close the file.

7. Bring up the Cloud Data Trunk:

```
ifdown ethP
ifup ethP
ifdown ethQ
ifup ethQ
```

8. Configure the DHCP_HOSTNAME to allow the management hypervisor to register itself with the DNS server:

```
vi /etc/sysconfig/network
DHCP_HOSTNAME=management_hypervisor_name
```

9. Add the DNS server IP address:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
DNS1=192.0.2.2
```

10. Reboot all compute nodes on the network to re-establish security group settings for the virtual machines running on the compute nodes.
11. Determine if you are using a be2net NIC driver:

```
# ethtool -i eth0
```

12. If you are using a be2net NIC driver, set the rx_frag_size value to 8192.
    a. Open the **be2net.conf** file in `/etc/modprobe.d/`.

       Create this file if it does not exist.
    b. Add the following line to the be2net.conf file:

       ```
       options be2net rx_frag_size=8192
       ```
    c. Save the file.
    d. Reboot the compute node.

IMPORTANT: If at any point you decide to run `service network restart`, you must reboot the compute nodes to re-establish security group settings for the virtual machines running on the compute nodes.

Next steps:

- Activate a compute node (page 105)

17 Compute node management

Once you have compute nodes or clusters created, you can bring them into CloudSystem for use in the cloud you are creating for your end users. Use the information in this chapter to manage the KVM compute nodes and ESX clusters in your virtual data center.

About Compute Nodes

A compute node provides the ephemeral storage, networking, memory, and processing resources that can be consumed by virtual machine instances.

CloudSystem supports two types of compute nodes:

- **ESX clusters**: Clusters are created in VMware vCenter Server. When the vCenter Server is registered and configured in the CloudSystem Console, clusters can be imported from vCenter Server and activated in the cloud.
- **KVM compute nodes**: KVM compute nodes are created manually. Once created, the Cloud Management Network enables the CloudSystem Console to see the KVM compute nodes. When the CloudSystem Console detects a compute node, it is automatically added to the Compute Nodes screen in an **Unknown** status.

Compute nodes in the cloud

Within a cloud environment, compute nodes form a core of resources. They supply the processing, memory, network, and storage that virtual machine instances need. When an instance is created, it is matched to a compute node with the available resources. A compute node can host multiple instances until all of its resources are consumed.

Managing compute nodes

Activating an ESX cluster or a KVM compute node performs the configuration required to bring the system into the cloud. This includes the following actions:

- **Activating an ESX cluster**: Verifies virtual switch settings and notifies the vCenter Server proxy appliance to start managing instances deployed on the cluster.

IMPORTANT: Do not activate an ESX cluster in more than one cloud.

- **Activating a KVM compute node**: Installs agents, identifies network interfaces, and verifies the operating system and the compute node status.

The **Compute Nodes** screen in the CloudSystem Console displays all available ESX clusters and KVM compute nodes, along with their resources. You can perform the following tasks from this screen:

- Import an ESX cluster from vCenter Server.
- Activate an ESX cluster or a KVM compute node.
- Deactivate an ESX cluster or a KVM compute node.
- Delete an inactive, previously imported ESX cluster or expire the DHCP lease on a KVM compute node.

The CloudSystem Portal contains a **Hypervisor** tab, which allows administrators to see all activated ESX clusters and KVM compute nodes, along with the number of instances attached to each.

Can I delete compute nodes from the cloud?

You can use the delete action to remove an imported ESX cluster, if it has been deactivated. Deleting an inactive ESX cluster removes it from the **Compute Nodes** overview screen, but does not affect

the ESX cluster itself, because it is managed in vCenter Server. See Deactivate a compute node (page 106), and Delete a compute node (page 107).

When the delete action is used on KVM compute nodes, the DHCP lease is expired and the compute node is no longer manageable from CloudSystem.

Understanding compute node data

You can click the ▸ icon next to an ESX cluster or KVM compute node on the overview screen to show all available data.

Two groups of horizontal graphs display when the compute data is expanded. The top set of graphs show the allocation usage of the instances. See Calculating the number of instances that can be provisioned to a compute node (page 105). The bottom set of graphs show the physical usage of the instances.

Allocation graphs

These graphs show the virtual size, which is the physical size multiplied by the oversubscription rate. For clusters, this is the aggregate value of all hypervisors in the cluster.

- CPU allocation: Amount of CPU cores designated for instances
- Memory allocation: Amount of memory designated for instances
- Storage allocation: Amount of compute storage designated for instances

Physical usage graphs

These graphs show the physical size information. For clusters, this is the aggregate value of all hypervisors in the cluster.

- CPU usage: Number of actual CPU cores consumed by instances within the last five minutes
- Memory usage: Amount of actual memory consumed by instances within the last five minutes
- Storage usage: Amount of actual compute storage consumed by instances within the last five minutes

When one or more virtual machine instances are attached to an ESX cluster or KVM compute node, you can click the instance link next to **Contains**. The link takes you to the Instances screen, where you can view the Instance details.

The **Dashboard** provides another view of compute node resources. See Interpreting the Dashboard data (page 114).

Adding compute nodes to the cloud

Compute nodes are added to the cloud in different ways, depending on the type of compute node you want to add.

ESX clusters appear on the **Compute Nodes** screen after you complete the following two steps:

- Register the management VMware vCenter Server. This action provides CloudSystem Foundation with the location and credentials of the vCenter Server managing the ESX cluster.
- Import a cluster. This action calls vCenter Server and retrieves information about an ESX cluster. The cluster is added to the Compute Nodes overview screen in an Unknown state. The first time a cluster is imported, the proxy appliance establishes communication between vCenter Server and the CloudSystem Console. The proxy appliance can support up to 12 ESX clusters. When more than 12 ESX clusters are imported, a new proxy appliance is spawned.

KVM compute nodes are issued a DHCP lease from the Cloud Management Network, and then they appear on the **Compute Nodes** screens in an Unknown state.

After an **Activate** action is performed, ESX clusters and KVM compute nodes are ready to host instances.

Calculating the number of instances that can be provisioned to a compute node

The maximum number of virtual machines that can be provisioned to a compute resource is based on the following:

- Amount of installed memory, available disk capacity, and number of CPU cores on the compute resource
- Flavor settings of the virtual machines to be provisioned
- Resource oversubscription, which is individually applied to the memory, disk, and CPU calculation

Table 11 (page 105) shows resource oversubscription rates so you can properly dimension the capacity of your compute resources based on virtual machine size requirements.

NOTE: These rates are hard coded in CloudSystem Foundation and cannot be changed.

Table 11 Resource oversubscription rates for KVM and ESX

Physical resource	Virtual resource	Physical to virtual oversubscription rate
1 CPU core	8 CPU cores	1:8
1 GB RAM	1.5 GB RAM	1:1.5
1 TB disk	1 TB disk	1:1

Import a cluster

Use this procedure to add an ESX cluster to the cloud. ESX clusters are imported from VMware vCenter Server.

Prerequisites

- vCenter Server is registered in Integrated Tools
- ESX cluster is created in vCenter Server.

Procedure 54 Importing an ESX cluster

1. From the main menu, select **Compute nodes**.
2. Select **Actions→Import**.

   The Import Cluster screen opens.
3. Select the vCenter Server you registered in Integrated Tools.
4. Select the datacenter.
5. Select the ESX cluster you want to import.
6. In the **Activate** field, click to toggle between Yes and No.
   - **Yes**: cluster is imported and then activated.
   - **No**: cluster is imported but is not activated. You can activate the cluster at a later time.
7. Click **Import**.

   To exit the action without adding the cluster, click **Cancel**.
8. Verify that the ESX cluster appears on the Compute Node overview screen. Clusters that were activated during the import action should have a green **OK** status. Clusters that were not activated should have a grey **Unknown** status.

Activate a compute node

Before being activated, ESX clusters imported from vCenter Server and KVM compute nodes appear on the Compute Nodes overview screen with a status of **Unknown**. Use the **Activate** action to add

ESX clusters and KVM compute nodes into the cloud. If the cluster or compute node does not appear on the overview screen, see Adding compute nodes to the cloud (page 104).

Prerequisites

- Minimum required privileges: Infrastructure administrator
- For ESX clusters:
  - ESX hypervisor hosts are created and configured in a cluster in vCenter Server. For more information, see VMware vSphere Documentation at VMware.
  - vCenter Server is registered on the **Integrated Tools** screen. See Register VMware vCenter Server (page 82).
- For KVM compute nodes:
  - Software, storage, and networking are installed and configured on the compute node hypervisor.
  - Space is allocated on the physical server where the hypervisor is running for the log files captured in the `/var/log/nova` directory.

NOTE: Instances that are not managed by CloudSystem consume resources and may cause oversubscription. If you plan to activate an ESX cluster or KVM compute node that is already hosting instances managed by other tools, you should first manually remove these instances using the same tools that you use to manage the instances. (This action cannot be performed using CloudSystem.)

Procedure 55 Activating a cluster or compute node

1. From the main menu, select **Compute Nodes**.
2. Select the ESX cluster or KVM compute node you want to activate.
3. Select **Actions→Activate**.
   - If activating an ESX cluster, then skip to step 4.
   - If activating a KVM compute node, first complete the steps below, then continue with step 4.
     - Enter the user name and password for the operating system running on the KVM compute node. These credentials are defined when the KVM compute node hypervisor is provisioned.
     - Enter the Cloud Data Trunk interfaces used to connect network devices to the KVM compute node. If there are multiple interfaces, separate them with commas. For example: `eth1, eth2`. See Networks in CloudSystem Foundation (page 19).
4. Click **Activate**.

   To exit without activating the ESX cluster or KVM compute node, click **Cancel**.
5. Verify that the ESX cluster or KVM compute node appears in a green active state on the **Compute Nodes** overview screen.

   NOTE: Do not activate an ESX cluster in more than one cloud.

Deactivate a compute node

Use this procedure to deactivate an ESX cluster or KVM compute node.

See About Compute Nodes (page 103).

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The compute node is activated.
- No virtual machine instances are deployed on the ESX cluster or KVM compute node. If instances are deployed, then you must remove the instances and redeploy them on a different compute node before you can deactivate the ESX cluster or KVM compute node. See Delete instance (page 109).

Procedure 56 Deactivating an ESX cluster or KVM compute node

1. From the main menu, select **Compute Nodes**.
2. Select the ESX cluster or KVM compute node you want to deactivate.
3. Select **Actions→Deactivate**.

   The Deactivate window opens.
4. Click **Deactivate**.

   To exit without deactivating the cluster or compute node, click **Cancel**.
5. Verify that the ESX cluster or KVM compute node appears in a gray Unknown state on the Compute Node overview screen.

See also

- Delete a compute node (page 107)
- Troubleshooting compute nodes (page 173)

Delete a compute node

Use this procedure to remove ESX clusters or KVM compute nodes from the Compute Nodes overview screen.

- **ESX clusters**: The delete action removes the cluster from the Compute Node overview screen. This action does not affect the ESX cluster itself, as it is managed in vCenter Server.
- **KVM compute nodes**: The delete action expires the DHCP lease for the compute node and removes it from the Compute Nodes screen.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- The compute node is deactivated. See Deactivate a compute node (page 106).

Procedure 57 Deleting an ESX cluster or KVM compute node

1. From the main menu, select **Compute Nodes**.
2. Select the ESX cluster or KVM compute node you want to delete.
3. Select **Actions→Delete**.
4. Click **Yes, Delete**.

   To exit the action without deleting an ESX cluster or KVM compute node, click **Cancel**.
5. With the filter set to **All statuses**, verify that the ESX cluster or KVM compute node was removed from the **Compute Nodes** overview screen.

18 Virtual machine configuration for compute services

Within CloudSystem Console, you can define "flavors" for the virtual machines deployed to the cloud. Flavors define the compute resources that can be assigned to each virtual machine. Also within the Console, you can do a few actions with virtual machine instances, such as restart and reboot an instance. However, you provision and deploy VMs through the CloudSystem Portal. See also Cloud service provisioning, deployment, and service management in CloudSystem Portal (page 116).

About virtual machine instances

Virtual machines instantiated in the CloudSystem Portal or by using the OpenStack API are visible in the CloudSystem Console. (See Cloud service provisioning and deployment in Enterprise (page 134).) Virtual machines instantiated in CloudSystem Enterprise are visible in the CloudSystem Console and the Cloud Service Management Console.

When an instance is launched using the CloudSystem Portal, it is started and available for use. You can view attributes of the instance on the **Instances** screen in the CloudSystem Console.

Managing virtual machine instances

From the **Instances** screen in the in the CloudSystem Console, you can perform the following actions:

- Create an image from a snapshot of an instance. This allows you to capture the attributes of the running environment of an instance and duplicate it for future use.
- Start an instance, if the instance is Suspended, Paused, or Stopped.
- Reboot an instance either with a soft reboot that restarts the instance software or with a hard reboot that forces a power cycle. Instances can be rebooted only when their state is Active, Shutoff, or Resize pending. If necessary, you can change the state in the CloudSystem Portal.
- Delete an instance. Instances can be deleted regardless of their state.

From the **Instances** tab in the CloudSystem Portal, you can perform additional actions on instances, including changing the state, editing, and resizing, among others.

Access the CloudSystem Portal by appending **/portal** to the Foundation appliance URL in your browser (for example, `https://192.0.2.0/portal`).

IMPORTANT: Do not use the CloudSystem Console or the CloudSystem Portal to change the state of virtual machines that were instantiated using the Enterprise Cloud Service Management Console.

CloudSystem Foundation does not propagate changes made to the instance state to CloudSystem Enterprise. Therefore, if you change instance states in Foundation, and then view the instance state in Enterprise, the state will differ from what is shown in the CloudSystem Console and Portal.

CloudSystem Console provides a limited set of state change actions. Cloud users have additional options. See Enterprise Information Library for more information.

Start instance

Use this procedure to start an instance.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- Verify the state of the instance to be started. The instance must have a state of **Suspended**, **Paused**, or **Stopped**. (Instances in a **Shutoff** state can be started using the **Reboot** action. See Reboot instance (page 109).)

Procedure 58 Starting an instance

1. From the **Instances** overview screen, select the instance by clicking its row.
2. Select **Actions→Start**.
3. A dialog appears with the name of the selected instance. Choose **Yes, Start** or **Cancel**.
4. Verify that the state of the instance becomes Active on the **Instances** overview screen.

Reboot instance

Use this procedure to reboot an instance.

IMPORTANT: Do not use the CloudSystem Console or the CloudSystem Portal to change the state of virtual machines that were instantiated using the Enterprise Cloud Service Management Console.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- Verify the state of the instance to reboot. The instance must have a state of **Active**, **Shutoff**, or **Resize Pending**.

Procedure 59 Rebooting an instance

1. Select the instance to reboot.
2. Select **Actions→Reboot**.

   A dialog appears with the name of the selected instance. The dialog provides you a choice: either a soft reboot, which performs a shutdown and restart of the virtual machine software, or a hard reboot, which forces a power cycle.
3. Choose **Yes, soft reboot** or **Yes, hard reboot**, or select **Cancel** to exit without making changes.
4. Verify that the state of the instance becomes Active on the **Instances** overview screen.

Delete instance

Use this procedure to remove unused or unwanted instances from the database. Deleting an instance deletes it from the compute node and removes the instance entry from the CloudSystem Foundation database.

Prerequisites

- Minimum required privileges: Infrastructure administrator

Procedure 60 Deleting an instance

1. Select the instance to delete. You can delete an instance regardless of its state.
2. Select **Actions→Delete**.

   A dialog displays the name of the selected instance.
3. To remove the instance from the **Instances** overview screen, select **Yes, delete**.

   To return to the previous screen with no changes made to the appliance, select **Cancel**.
4. With the filter set to **All statuses**, verify that the instance was deleted from the **Instances** overview screen.
5. Verify that the CloudSystem Portal is updated when instances are deleted from CloudSystem Console.

About Flavors

An Infrastructure administrator determines the flavors available for assignment to virtual machine instances. A *flavor* defines the size of compute resources (number of virtual CPUs, memory and storage capacity) that can be assigned automatically to virtual machine instances in a cloud configuration. The flavor options provide flexibility when the Cloud administrator initially sizes compute resources for virtual machine instances.

Flavors in the cloud

The Infrastructure Administrator creates flavors from the **Flavors** screen of the CloudSystem Console. A cloud user can select a flavor when creating a new instance in the CloudSystem Portal. The available flavors populate the **Flavor** drop down list in the **Launch Instance** window.

Manage flavors

You can add and delete flavors in the CloudSystem Console. After a flavor is created, it cannot be changed.

Add Flavor

Prerequisites

- Minimum required privileges: Infrastructure Administrator

Procedure 61 Adding a flavor

1. From the main menu, navigate to **Flavors**.
2. Select **Actions→Add**.
3. Enter the data. Select "Help on this page" in the CloudSystem Console for more information.
4. Click **Add** to complete this action.
5. Verify that the new flavor appears on the **Flavors** overview screen.

Procedure 62 Adding multiple flavors in one action

1. From the main menu, navigate to **Flavors**.
2. Select **Actions→Add**.
3. Enter the data.
4. Click **Add +** to save the flavor and reset the form for the next flavor.
5. Repeat steps 3 and 4 until you are finished adding multiple new types, then click **Cancel** to dismiss the **Add** screen.
6. Verify that the new flavors appear on the **Flavors** overview screen.

Can I delete a flavor that was used to create an instance?

You can delete a flavor if the flavor has not been associated with a currently running virtual machine instance. You can see the number of instances associated with a flavor on the **Flavors** overview screen in the **Instances** column.

If you want to delete a flavor and the number of associated instances is one or more, do one of the following:

Procedure 63 If you want to delete a flavor because you no longer need the instances using the flavor

1. Make sure that the instances are no longer needed before proceeding.

   In CloudSystem Foundation and CloudSystem Enterprise, information can be associated with instances that can help you can determine ownership and use of the instances.
2. From the **Instances** screen, delete all instances associated with the flavor.
3. From the **Flavors** screen, delete the flavor that is no longer associated with any instances.
4. Verify that the flavor was deleted from the **Flavors** overview screen.

Procedure 64 If you want to delete a flavor because you are assigning a new flavor to one or more instances

1. Access the CloudSystem Portal by entering `https://`*`Foundation_IP`*`/portal` in your browser.
2. Open the CloudSystem Portal and select **Instances** in the **Project** tab.
3. Select the instance associated with the flavor you want to delete, and click **More**.

4. Select **Resize Instance**, and select a new flavor to associate with the instance.
5. From the **Flavors** screen in the CloudSystem Console, delete the flavor that is no longer associated with any instances.
6. Verify that the flavor was deleted from the **Flavors** overview screen.

Delete Flavor

Use this procedure to delete a flavor from the CloudSystem Console.

You can delete a flavor only when it is not associated with an instance. See Can I delete a flavor that was used to create an instance? (page 110)

Prerequisites

- Minimum required privileges: Infrastructure Administrator
- The flavor to be deleted is not associated with an instance.

Procedure 65 Deleting a flavor

1. From the main menu, select **Flavors**.
2. Select the row of the flavor to remove.
3. Select **Actions→Delete**.
4. To complete the deletion, click **Yes, delete**.

   To exit without deleting the flavor, click **Cancel**.
5. Verify that the flavor was deleted from the **Flavors** overview screen.

19 Monitor resource use and allocation in CloudSystem Console

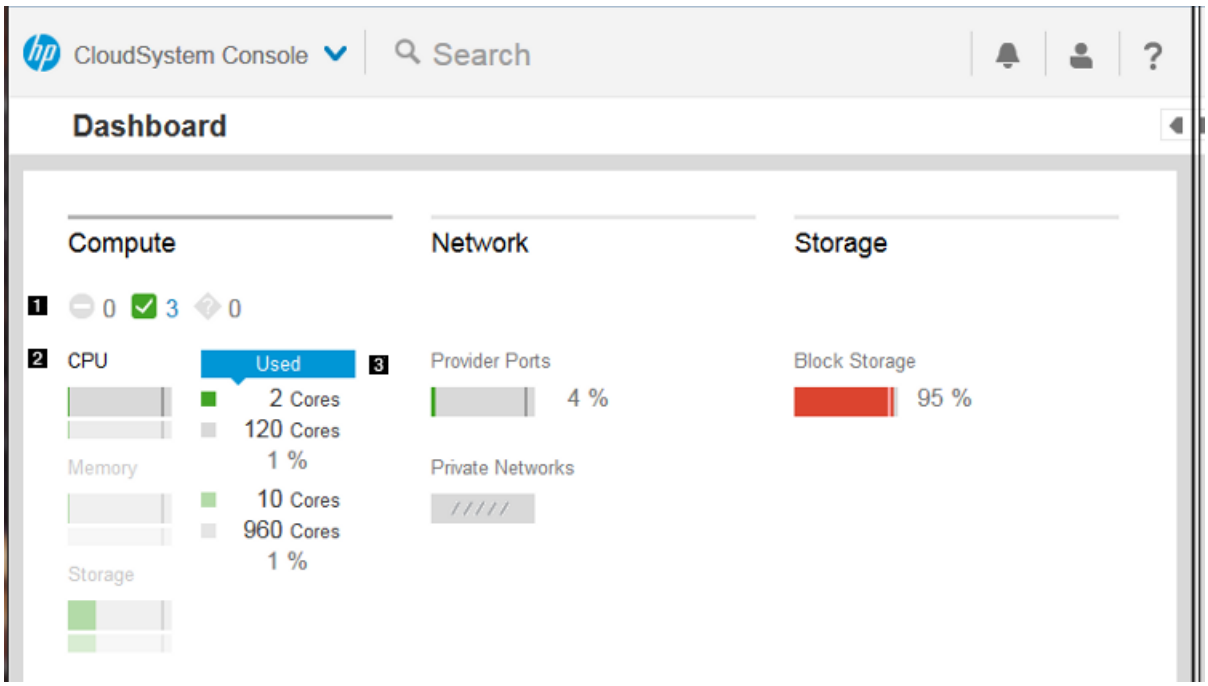
When you first enter CloudSystem Console, you see the Console Dashboard where you can quickly obtain an overall understanding of the state of cloud resources. Use the information in this chapter to learn how to interpret the Dashboard data display.

About the Console Dashboard

The Dashboard provides a visual representation of the health and status of your compute, network and storage resources. Use the top section to monitor resource usage and availability. Use the bottom section to view the creation and deletion of virtual machine instances, network ports, and storage volumes.

The graphs display the resource pool for the entire group of compute nodes, networks or storage resources.

Figure 10 Dashboard of physical and virtual resource allocation and usage



1 **Status icons** show the combined status of all compute nodes. Click a status icon to navigate to the Compute Node overview screen in the Console, where you can view more details.

2 **Usage and allocation graphs** provide a visual representation of usage or allocation of physical or virtual resources consumed within the last five minutes.

The gray bar represents 100% of the value possible, the colored area represents current activity as a percentage of the total possible, and the thin vertical line on the right side of the gray bar represents the utilization threshold, for which the default value is 90%. On approaching the threshold, the current activity color indicator will turn red.

In each resource area, hovering over the graphical bars reveals current numeric data about the physical and virtual resources allocated and in use for compute resources, networks and storage.

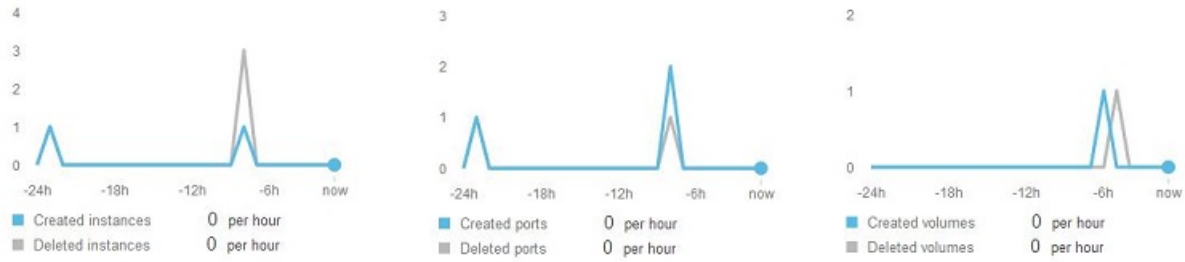
In this example, the hover is over CPU in the Compute area of the Dashboard. Therefore, the CPU graph is shown in deeper hues, and core data is displayed alongside the graphical bars with the percentage of usage overall of physical and allocated virtual resources.

3 Changing the focus to hover over the numeric values reveals blue labels for each value, which have the following general meanings:

- **Used:** The total amount of physical resource in use by all managed virtual machines.
- **Physical total:** The combined amount of physical resource available for use in the virtual environment.
- **Allocated:** The amount of physical resource that is allocated for use to each virtual machine.
- **Virtual limit** the total amount of available physical resource multiplied by the oversubscription rate applied to that resource.

See also Calculating the number of instances that can be provisioned to a compute node (page 105).

Figure 11 Activity graphs



The bottom section of the Dashboard contains graphs that track the create and delete activities of the components that consume the resources. The graph represents activity over a 24-hour period. The values below the graph change as you hover left to right over the graph. The blue graph line represents all created components and the gray line represents all deleted components.

See also Interpreting the Dashboard data (page 114)

Dashboard status indicators

The Dashboard communicates the state of compute resources through shape, color, and data.

Status icons

Click the Compute Node status icons to navigate away from the Dashboard to the Compute Node overview screen. For information on the meaning of the icons, see Status and severity icons (page 32).

If no resources are defined or if no resource instances are detected with a particular status (indicated by the number zero), the associated icon is nearly colorless (very pale gray).

Graphs

Dashboard graph colors provide a quick way to visually interpret the data being reported.

Table 12 Dashboard graph colors

Color	Indication
Green	A healthy status
Yellow	An event has occurred that might require your attention
Red	A critical condition that requires your immediate attention
Medium gray	Represents the *total possible usage or allocation* of the resource to virtual machines.
Light gray	Represents the *total physical or virtual resource pool available* to virtual machines to use.

Interpreting the Dashboard data

Data refresh

Dashboard information for both the top and bottom graphs is refreshed every 15 seconds.

The graphs along the bottom of the Dashboard represent dynamically refreshed data presented in two ways:

- **Just-in-time data**: Every 15 seconds, the data point on the right side of the graph (labeled **now**) is updated, representing the resources that have been successfully created or deleted since the top of the current hour. For example, at 1:15pm, the **now** indicator shows the resources created or deleted in the 15 minutes since 1:00pm.
- **Historical data**: The remainder of the graph shows the hourly totals for the 23 hours prior to the current hour. At the top of each hour, the oldest data point is dropped and the remaining data points shift to the left. A new **now** indicator is started with a value of zero. This shift provides a consistent view of historical activity.

Compute

Compute nodes host virtual machine instances, providing the CPU, memory and storage resources that instances require. The Dashboard displays horizontal graphs that indicate the amount of compute resources consumed by all instances across all compute nodes. A green graph indicates that there are compute nodes available for instance consumption.

When a resource enters a critical state, then 90% or more of the resource has been consumed. The horizontal usage graph color changes from green to red when a critical state is reached. You should plan to add additional compute nodes when a usage graph enters a critical state.

Compute node storage differs from the other storage type shown on the Dashboard. Compute node storage is the amount of space an instance consumes when it is created. Compute node storage cannot be added from the Storage area of the CloudSystem Console. You must add additional compute nodes to provide additional compute node storage.

The Compute graph on the bottom portion of the screen tracks the number of instances created or deleted during a 24-hour period. These instances could be created in Foundation, Enterprise or from REST APIs. The graph shows the total number of all instances created or deleted, regardless of their point of origin. You can use this information to track activity and use the results to plan for additional resource needs.

Network

The Dashboard displays information about the availability of provider and private network IP addresses. Provider networks enable you to provision existing data center networks to the cloud. Private networks enable groups of end-users to exclusively share virtual machine instances provisioned inside the cloud using VLANs that you select for that purpose.

The Provider ports horizontal graph shows the amount of Provider Network IP addresses that are assigned to instances. A port is defined as a specific IP address, created from the subnet allocation pool on the Provider Network screen.

The Private network horizontal graph shows the number of Private network IP addresses that are assigned to instances. Private network VLAN IDs and ranges are defined on the Private Network screen of the CloudSystem Console. The OpenStack Networking service assigns VLANs from this pool to Private Networks when they are created by end users using the CloudSystem Portal.

A green graph indicates that network IP addresses are available to attach to instances. When network availability reaches a critical state (90% or more of the available network IP addresses are consumed), then the graph changes to red. You should plan to add additional networks when a usage graph enters a critical state. See Add Provider Network (page 74) and Add VLAN IDs (page 76) (for Private Network assignments).

The Network graph at the bottom of the screen tracks the number of provider and private networks created or deleted over a 24–hour period. You can use this information to track activity and use the results to plan for additional resource needs.

Storage

The Storage section of the Dashboard shows the overall capacity and usage of the storage systems registered for block storage use. Block storage is the storage used for the data disks attached to instances.

The usage graph reflects the consumption of block storage by all sources. When the block storage consumption enters a critical state (90% or more of the available capacity), then the graph changes to red. You should plan to add additional storage resources, if block storage resources enter a critical state. See Add Block Storage Drivers (page 89).

You can use the volume create and delete activity graphs at the bottom of the screen to help plan for additional resource requirements.

Part IV Cloud service provisioning, deployment, and service management in CloudSystem Portal

20 Provision a cloud in Foundation

CloudSystem interfaces with the ESX cluster or KVM compute node to launch virtual machine instances and connect the networks. After the necessary cloud resources are configured in the CloudSystem Console, you can log in to the CloudSystem Portal and deploy virtual machine instances to the cloud.

To access the CloudSystem Portal, open a new browser tab and copy the CloudSystem Foundation address, then modify it by appending `/portal`. For example: `https://192.0.2.2/portal`.

NOTE: When local logins are enabled, Infrastructure administrators can access the CloudSystem Portal using their CloudSystem Console credentials (user name and password).

See About user roles (page 52) for more information.

Launching a virtual machine instance in the CloudSystem Portal

Before you launch an instance, complete the following CloudSystem Portal tasks so that you will be able to enter all the instance details in the **Launch Instance** window.

☑	Task	Why it matters	Procedure
	Create security rules for VMs running on KVM compute nodes and assign them to security groups	When a user launches an instance, a security group is assigned to the instance to define the ways in which the instance can be accessed, for example using `ssh`. A security group can have TCP and UDP rules for access to certain ports. It can also have ICMP rules, which specify a type and a code rather than a port. The security rules also dictate which remote IP addresses can connect to and from the instance. Security groups for VMs running in an ESX cluster must be set in vSphere vShield Manager when you configure the cluster.	Create a security group (page 118)Create a key pair (page 119)
	Create key pairs	A key pair provides a secure way to log in to an instance. You can create and save a key pair, then associate it with an instance when the instance is created.	Configuring security groups for instances in an ESX cluster (page 98)
	Define flavors	The flavor defines the amount of resources consumed by the instance. You can add additional flavors if you need a different resource consumption scale.	Add Flavor (page 110)
	Create images	The image defines the operating system. You can add additional images, which are used to boot instances in the cloud.	Image management (page 84)
	Add networks	Provider or Private networks allow instances to communicate in the cloud.	Network configuration (page 73)

There are two ways to deploy, or launch, instances in the CloudSystem Portal.

- You can launch an instance from the **Instances** screen

  Select **Launch instance** and add instance details in the Launch Instance window.

- You can launch an instance from the **Images** screen.

  Create an image, then select the **Launch** button next to that image and add the instance details in the Launch Instance window.

You can connect to the instance console from the **More** button to the right of the instance. Use **Back** to exit the console when finished.

The CloudSystem Console is built on OpenStack Horizon technology. For more information on the Horizon architecture and how to use the portal features from an end user's perspective, consult the *OpenStack Operations Guide* for Havana release.

Create a security group

Prerequisites

- Minimum required privileges: Cloud User

Procedure 66 Creating a security group

1. Log in to the CloudSystem Portal.
   a. Type the FQDN or the IP address of your CloudSystem Console in a new browser window.
   b. Add **/portal** to the end of the FQDN or IP address. Example:
   `https://192.0.2.0/portal`
2. Click the **Project** tab.
3. Select your project from the drop down list.
4. Click **Access & Security** from the left menu.
5. Click **Security Groups**.
6. Click **Create Security Group**.
7. Click the **Create Security Group** button.
8. Enter a name for the security group. Example: SGSSHandPing
9. Enter a description for the security group.
10. Click **Create Security Group**.
11. Verify that the new security group appears on the Security Group screen.
12. Click the **Edit Rules** button to the right of the security group you just created.
13. Click **Add Rule**.
14. Fill in the fields that define the rules you want to apply. For example:
    - To create a rule that allows ssh traffic, under Rule, select SSH rule at the bottom of the list.
    - To create a rule that allows ping traffic, under Rule, select All ICMP rule.
    - To create a rule that allows remote Windows desktop access, under Rule, select All ICMP, SSH, RDP
15. Associate a security group to this rule.
16. Click **Add**.

Create a key pair

Prerequisites

- Minimum required privileges: Cloud User

Procedure 67 Creating a key pair

1. Click the **Project** tab.
2. Click **Access & Security** from the left menu.
3. Click the tab for **Keypairs**.
4. Click **Create Keypair**.
5. Enter a key pair name.
6. Click **Create Keypair**.

   Your browser will give you the opportunity to open and save the key pair.

Create a Private network

Prerequisites

- Minimum required privileges: Cloud User

Procedure 68 Creating Private networks for instances

1. Log in to the CloudSystem Portal.
   a. Type the FQDN or the IP address of your CloudSystem Console in a new browser window.
   b. Add **/portal** to the end of the FQDN or IP address. Example:
   `https://192.0.2.0/portal`
2. Click the **Project** tab and select a project from the drop down list.
3. Click **Network Topology** on the left menu.
4. Click **Create Network**.
5. Assign a unique name to the network.
6. Click **Admin State** if you want to make this network immediately available to users. If you need to configure additional networking infrastructure before allowing users to have access to this network, then leave this box unchecked.
7. Click the **Subnet** tab.
8. Assign a unique subnet name.
9. Assign a network address.
10. Leave the Gateway IP address empty, which allows the appliance to assign the IP address.
11. Click the **Subnet Detail** tab.
12. Click **Enable DHCP**.
13. Enter the allocation pools. This is the list of IP addresses that can be given to new instances.
14. Enter the name of your DNS server.
15. Leave the Host Routes field empty.
16. Click **Create**.
17. Verify that the Private network appears on the Network Topology screen.

Launching an instance using CloudSystem Portal

Prerequisites

- Minimum required privileges: Cloud User
- Security groups and security rules are defined.
- At least one Provider or Private Network is created.
- At least one image or one snapshot is uploaded.

Procedure 69 Launching an instance using CloudSystem Portal

1. Log in to the CloudSystem Portal with Cloud User credentials.
   The portal opens to the **Project** tab.
2. A default project is shown. Choose a different project from the drop down selector if needed.
3. Click **Images & Snapshots** from the left menu.
   The Images screen displays.
4. Find the image you want to use and click the **Launch** button.
   The Launch screen displays.
5. For **Availability Zone**, leave the default **nova** selected.
6. In the **Instance Name** field, enter a name for the instance.
7. From the **Flavor** drop down box, select a flavor.
8. In the **Instance Count** field, enter the number of instances to launch.
9. From the **instance boot source** drop down box, select a source.
   The supported options are **boot from image** and **boot from snapshot**.
10. From the new field added below the instance boot source field, select an image or snapshot.
11. Click the **Access & Security** tab.
12. Select a key pair.
    The key pair provides SSH access to an instance.
13. Create a new administrator password for the operating system administrator account.
14. Confirm the password.
15. Select a security group.
    You must attach a security group with rules to SSH or ping instances, or you will not be able to reach the instance after it is created.
16. Click the **Network** tab.
17. Drag the network(s) you want to associate with the instance up to the **Selected Networks** field.

    NOTE: Do not select the External network. This network should never be directly connected to an instance. See About the External Network (page 77).

18. Click **Launch**.
19. Verify that the instance appears on the Instances screen. If multiple instances were launched, verify that all instances appear on the **Instances** screen.

Create a volume to attach to an instance

Prerequisites

- Minimum required privileges: Cloud User

Procedure 70 Creating a volume to attach to an instance

1. Log in to the CloudSystem Portal.
   a. Type the FQDN or the IP address of your CloudSystem Console in a new browser window.
   b. Add **/portal** to the end of the FQDN or IP address. Example:
      `https://192.0.2.0/portal`
2. Click the **Projects** tab.
3. Click **Volume** from the left menu.
4. Click **Create volume**.
5. Enter a unique volume name.
6. Enter an optional volume description.

7. Select a volume type. These are populated from the volume types entered in the CloudSystem Console.
8. Enter a size.
9. Select a volume source. You can select **image** here if you plan to use this as a boot volume.
10. Click **Create volume**.
11. Verify that the volume is listed on the Volumes screen.
12. Select the volume and click **Edit attachments**.
13. Select the instance to attach.
14. Enter a name for the device. This field looks like it is already filled in, but you need to make sure to enter a device name.
15. Click **Attach Volume**.

21 Monitor and manage infrastructure services in CloudSystem Portal

An Infrastructure administrator created in the CloudSystem Console can view and manage all resources in the Console.

Using the same user name and password, an Infrastructure administrator can log into the CloudSystem Portal and view and manage all resources in the Portal using the **Admin** tab.

NOTE: The Infrastructure administrator must log into the CloudSystem Console at least once before logging into the Portal.

A cloud administrator created in the CloudSystem Portal can also view and manage all resources in the Portal. However, the cloud administrator can log into the CloudSystem Console only if the cloud administrator has a user account in the CloudSystem Console.

Monitoring allocation and usage in CloudSystem Console

From the **Admin** tab, you will be able to view allocation limits and usage for all compute resources made available to deploy to a cloud as a service.

From the **Project** tab, you can view allocation limits for selected projects, and use the time selector to view usage over a specified period of time.

The CloudSystem Console is built on OpenStack Horizon technology. For more information on the Horizon architecture and how to use the portal features from an end user's perspective, consult the *OpenStack Operations Guide* for Havana release.

Part V Understanding CloudSystem Enterprise

22 About CloudSystem Enterprise

HP CloudSystem Enterprise expands on CloudSystem Foundation to automate the integration of servers, storage, networking, security, and monitoring capabilities throughout the infrastructure service delivery lifecycle of a virtualized data center. Through the addition of HP CSA, Enterprise offers additional design tools and provider integration, and with the Marketplace Portal, users have secure access to these services.

About the Enterprise appliance

Enterprise and Foundation are separate virtual appliances. However, all appliance management tasks are performed through the Foundation CloudSystem Console and all OpenStack functionality included in Foundation is available to Enterprise. See also Manage the Foundation appliances (page 46).

To account for the operation of the Foundation software underlying Enterprise, consider the maximum supported configuration for Foundation appliance when planning an Enterprise cloud. See Maximum supported configuration values for each CloudSystem (page 71).

HP CSA maps user roles through membership in LDAP groups configured through the LDAP service for the organization. HP CSA does not directly manage the creation or maintenance of individual users. As the HP CSA administrator creates organizations within HP CSA, the corresponding LDAP group membership must exist or be created.

When users log in, LDAP authenticates login credentials and verifies the appropriate role through group membership. LDAP directories must be pre-configured for the access process to function correctly in HP CSA.

See also Logging in and changing the default HP CSA and Marketplace Portal password (page 128).

Enterprise in the cloud

The **Enterprise appliance** contains the following components:

- **HP Cloud Service Automation (HP CSA)** and its user interface the **Cloud Service Management Console** orchestrate the deployment of compute and infrastructure resources and complex multi-tier application architectures. HP CSA integrates and leverages the strengths of several HP data center management and automation products, adding resource management, service offering design, and a customer portal to create a comprehensive service automation solution.

  The HP CSA lifecycle framework, and its features for leveraging resources, help you map cloud fulfillment infrastructure into reusable automated resource offerings.

  - The **Marketplace Portal** in HP CSA provides a customer interface for requesting new cloud services and for monitoring and managing existing services. Subscriptions are available at multiple price points, as defined by the subscription owner.
  - The **Topology Designer and Sequential Designer** are the HP CSA graphical service design and content portability tools. The designs created through both designers are presented as service offerings that Marketplace Portal users can select and provision. Topology Designer is used to create infrastructure service designs. Sequential Designer is used to create more complex application service designs.

    Topology Designer also supports HP Operations Orchestration (OO) callouts for pre- and post- compute node provisioning.

See the HP CSA documentation at Enterprise Information Library.

Multitenancy in Enterprise

Configure Enterprise and Foundation to enable multitenancy before using HP CSA to deploy offerings.

Refer to Supported console operations on the CloudSystem appliances (page 199) and the *Multitenancy in HP CloudSystem Foundation and Enterprise* white paper in the Enterprise Information Library for configuration details.

23 Install Enterprise

Before installing Enterprise

When you install Enterprise, a new virtual appliance is created. Before you begin the installation, make sure you have the following prerequisites in place.

- Minimum required privileges: Infrastructure administrator
- CloudSystem Foundation is fully installed and first time setup is complete.
- You do not plan to make any changes to the CloudSystem Foundation network configuration. If you change the Foundation network configuration after Enterprise is installed, you must then uninstall and reinstall Enterprise.
- If you plan to enable strong OpenLDAP or Active Directory certificate validation for authentication to the CloudSystem Portal, you have reviewed the steps in the Enabling strong certificate validation in the CloudSystem Portal (page 189).

  Strong certificate validation may require a change to the alternate DNS server in the CloudSystem Foundation base appliance. Any changes to the Foundation network configuration must be made before Enterprise is installed.
- In an ESX configuration, the Enterprise OVA is converted to a template and added to the cluster datastore in vCenter Server. You can find this OVA in the **CloudSystem-Enterprise-ESX** installation tar file.
- In a KVM configuration, the Enterprise qcow2 image is saved to a Linux workstation. You can find this qcow2 image in the **CloudSystem-Enterprise-KVM** installation tar file.
- You are using a supported browser. See Browser requirements (page 34).
- You have selected an IP address and Fully Qualified Domain Name (FQDN) for the Enterprise appliance and registered it with the DNS server.
- You have the user name and password for OO Central. This is the same user name and password for the CloudSystem Console.

About IP address types

Enterprise and Foundation must use the same IP address conventions. If Foundation was configured to support DHCP address assignments, this configuration will apply automatically to Enterprise. If Foundation was configured to support static IP addresses, you must enter an IP address for the new Enterprise virtual appliance.

Install the Enterprise appliance

Use this procedure to install CloudSystem Enterprise.

Prerequisites

- Foundation is fully installed.
- In an ESX configuration, the Enterprise OVA is added to the datastore that supports the management cluster in vCenter Server.
- In a KVM configuration, the Enterprise `qcow2` image is saved to the Linux or Windows server where you ran `csstart` to install the Foundation base appliance.
- You are using a supported browser.

  See the "CloudSystem installation prerequisites" chapter of the *HP CloudSystem 8.0 Installation and Configuration Guide* in the Enterprise Information Library.
- You have selected an IP address, if using static IPs, and registered the FQDN for the Enterprise appliance with the DNS server.

Procedure 71 Installing CloudSystem Enterprise

1. From the main menu, select **Enterprise**.
2. Click **Actions→Install CloudSystem Enterprise**.
3. Review the installation instructions, then click **Next**.

   To exit any action without installing Enterprise, click **Cancel**.
4. Enter the Enterprise appliance host name and static IP address, then click **Next**.
5. Enter Operations Orchestration credentials.
6. Click **Install**.

   To exit the action without installing Enterprise, click **Cancel**.
7. Verify that the Enterprise appliance was created. The name of the virtual machine where the Enterprise appliance is running is automatically designated based on the management hypervisor hostname (ESX or KVM). For example, if the management hypervisor host name is **my-host-name.example.com** then the Enterprise appliance name is **my-host-name**.
   - If installed on ESX, confirm the Enterprise appliance is listed in vCenter in the cluster.
   - If installed on KVM, log in to the management hypervisor and enter the command

     ```
     virsh list --all
     ```

     Enterprise will be listed along with the base appliance, SDN controller and network node appliances.

All existing Foundation functionality will continue to be available. Enterprise appliance details can be viewed in Foundation on the **Enterprise** screen.

24 Enterprise appliance management

Managing the Enterprise appliance

You can install and access **Enterprise** from the main menu in the CloudSystem Console. When you visit the screen before Enterprise is installed, a list of prerequisites is provided to help you prepare for the installation. After Enterprise is installed, two new panels appear on the screen:

- **Tools**: Access links to HP CSA and Marketplace Portal
- **Configuration**: Edit the user name and password for Operations Orchestration Central

Table 13 CloudSystem Enterprise

Tool	Used in Enterprise to...	How to launch
HP CSA	Manage the deployment of compute and infrastructure resources and complex muli-tier appliance architecture	Click the Cloud Service Management Console link on the **Enterprise** pane of the **Enterprise** screen
Marketplace Portal	Display offerings that can be purchased and applied to a cloud environment	Click the Marketplace Portal link on the **Enterprise** pane of the **Enterprise** screen

About Enterprise appliance management tasks

When you install Enterprise, all Foundation functionality is still available by using the CloudSystem Console. Use the console to perform all Enterprise appliance management tasks.

About Operations Orchestration Central credentials

You can edit the Operations Orchestration Central login credentials from the **Credentials** pane on the Enterprise screen. These credentials are set to the CloudSystem Console first time login credentials by default.

About instances provisioned by Enterprise

When virtual machine instances are provisioned in Enterprise, they appear in the CloudSystem Console on the Instances screen and in the CloudSystem Portal on the Instances screen. You should use an easy to recognize name for virtual machine instances provisioned in Enterprise to help you distinguish them from virtual machine instances provisioned in Foundation.

IMPORTANT: Do not modify a virtual machine instance provisioned by Enterprise from the CloudSystem Portal. Changing instances that were provisioned in Enterprise outside the Enterprise appliance will result in irreversible errors.

Logging in and changing the default HP CSA and Marketplace Portal password

To log in to HP CSA, from the CloudSystem Console main menu, select **Enterprise**. Click the links in the **Tools** pane to open the Cloud Service Management Console or Marketplace Portal.

You can also open a new browser tab and copy the CloudSystem Enterprise IP address, then modify it by appending `/csa` or `/marketplace`. For example:
`https://`*`Enterprise_IP_address`*`/csa`
`https://`*`Enterprise_IP_address`*`/marketplace`

Log in to Enterprise using the default credentials in the following table.

Cloud Service Management Console	Marketplace Portal
User name: `admin`	User name: `consumer`
Password: `cloud`	Password: `cloud`

Use the following procedures to change the password of the default user names used to log in to the Cloud Service Management Console and the Marketplace Portal.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- Enterprise is installed. See Install the Enterprise appliance (page 126).
- You have access to the Enterprise appliance console using the hypervisor console.
  See Enable console access and set the password (page 199).

Procedure 72 Changing the default HP CSA admin password

1. Log in to Enterprise appliance console using the hypervisor console.
2. Go to the folder `/ci/usr/local/hp/csa/scripts`.
3. Run the following command and specify a new password in *<new_Password>*.

   ```
   /ci/usr/local/hp/csa/openjre/bin/java -jar passwordUtil.jar encrypt <new_Password>
   ```
4. Note the passwords that are displayed. The original password is the new password you entered in step 3.

   original: *<new_Password>*

   encrypted: *<encrypted_new_Password>*
5. Edit the file `/ci/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/deployments/csa.war/WEB-INF/classes/csa.properties`.
6. Search for a line similar to:

   ```
   securityAdminPassword = ENC(3oKr9eADA7bE53Zk2t9wIA==)
   ```
7. Replace the password to the right of the equal sign with the *<encrypted_new_password>* from step 4.
8. Save the `csa.properties` file.
9. Restart the HP CSA service by entering:

   ```
   service csa restart
   ```

Procedure 73 Changing the default Marketplace Portal consumer password

1. Log in to Enterprise appliance console using the hypervisor console.
2. Go to the folder `/ci/usr/local/hp/csa/scripts`.
3. Run the following command and specify a new password in *<new_Password>*.

   ```
   /ci/usr/local/hp/csa/openjre/ bin/java -jar passwordUtil.jar encrypt <new_Password>, SERVICE_CONSUMER,ROLE_REST,enabled
   ```
4. Note the passwords that are displayed. The original password is the new password you entered in step 3.

   original: *<new_Password>*

   encrypted: *<encrypted_new_Password>*

5. Edit the file `/ci/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/deployments/idm-service.war/WEB-INF/classes/csa-consumer-users.properties`.
6. Search for a line similar to:

   ```
   consumer=ENC(UUtPxLUMMJHjofhYVm47Sl3jsbUBs8/8LP6lW6bHT80+PFP6sV1u0Q==)
   ```

7. Replace the password to the right of the equal sign with the *<encrypted_new_password>* from step 4.
8. Save the `csa-consumer-users.properties` file.
9. Restart the HP CSA services by entering:

   ```
   service csa restart
   service mpp restart
   ```

Update the Enterprise appliance

Use these procedures to install an update for the Enterprise appliance. These procedures do not install an update for Foundation appliances. To do that, see Update Foundation appliances (page 48).

The amount of time required for the download depends on the components in the update and the speed of your network connection.

IMPORTANT: When the update begins, non-critical services on the appliance are stopped, including HP Cloud Service Automation and HP Operations Orchestration. (Operations Orchestration work flows are not accessible during the update.) Critical services, such as the database and update services, are not stopped. If the update installation fails, the appliance reverts back to its previous state and is restarted.

Prerequisites

- Minimum required privileges: Infrastructure administrator
- Enterprise is installed. See Install the Enterprise appliance (page 126).
- HP recommends that you create and download a backup file before updating the appliance. Information about backing up and restoring HP CloudSystem is provided in a white paper available at Enterprise Information Library.

Procedure 74 Updating the Enterprise appliance: Downloading the update file to your local computer

1. From the main menu, select **Enterprise**.
2. Select **Actions→Update Enterprise appliance**.

   The Update CloudSystem Enterprise screen is displayed.
3. Determine if other users are listed on the **Update CloudSystem Enterprise** screen as currently logged in to the appliance and, if necessary, inform them of the pending update.
4. Click “updates” in the line that reads “Go to hp.com for latest updates”.
5. Locate the CloudSystem images for the appliance. Update images are encrypted files with a `.bin` extension.
6. Download the new image file to your local computer.

IMPORTANT: Once you have downloaded the file to your local computer, ensure there are no validation errors showing on the **Update CloudSystem Enterprise** screen.

You are now ready to do one of the following.

- Upload the update file and install it at a later time.
- Upload the update file and install it immediately.

Procedure 75 Updating the Enterprise appliance: Uploading an update file and installing it at a later time

You must have at least 2 GB of space available on the appliance before proceeding.

1. To move the image file to the appliance, do one of the following:
   - Drag the image file from a folder on your local computer and drop it in the box on the **Update CloudSystem Enterprise** screen.

     NOTE: Some versions of Microsoft Internet Explorer do not support this method.

   - Click **Browse**, browse to the image file, and select it.
2. Click **Upload only**.

   The appliance validates the image, and details of the pending update are displayed on the **Update CloudSystem Enterprise** screen.

   If the image file is invalid, or if there is insufficient disk space, the appliance deletes the image file and displays the errors. Errors are also saved in `/updatelogs/update.log`. To download a new image file, see Downloading the update file to your local computer.
3. Once you are ready to install an uploaded image file:
   a. Return to the **Update CloudSystem Enterprise** screen. (**Enterprise→Actions→Patch Enterprise product**).
   b. Examine the "File" name line.

      If the image you previously uploaded is not listed, then browse to select it.
   c. Proceed with step 2 in Uploading and installing an update file immediately.

Procedure 76 Updating the Enterprise appliance: Uploading and installing an update file immediately

1. To move the image file to the appliance, do one of the following:
   - Drag the image file from a folder on your local computer and drop it in the box on the **Update CloudSystem Enterprise** screen.

     NOTE: Some versions of Microsoft Internet Explorer do not support this method.

     Click **Browse**, browse to the image file, and select it.
2. Click **Upload and install**.

   If this is the first time the image is being uploaded, the appliance validates the image and details of the pending update are displayed on the **Update CloudSystem Enterprise** screen.

   If the image file is invalid, or if there is insufficient disk space, the appliance deletes the image file and displays the errors. Errors are also saved in `/updatelogs/update.log`. To download a new image file, see Downloading the update file to your local computer.
3. Follow the "Release notes" link and read them to ensure that you understand the requirements of the update.

   NOTE: Save the *Release Notes* for future reference because when the download starts you will not be able to access the *Release Notes*.

4. Click **Continue**.

   The **CloudSystem Console License** screen appears.
5. To accept the license, click **Agree**.

   The **Update CloudSystem Enterprise** screen is displayed.

6. Click **OK**.

   CloudSystem services are stopped, the console is locked, and progress of the upgrade is displayed on a status screen. When the update process completes, the Enterprise appliance restarts. Depending on the components in the update, the appliance might automatically reboot when the update is complete.

7. When the update completes and the console displays the login screen, log in and verify the new CloudSystem version information on the **Enterprise** screen. You can also navigate to the Activity screen from the main menu to check appliance statuses after the update.

Uninstall the Enterprise appliance

Use this procedure to uninstall CloudSystem Enterprise.

IMPORTANT: After uninstalling Enterprise, all existing Foundation functionality will continue to be available. You can continue to use the **Dashboard**, **Settings** and **Compute Nodes** screens in the CloudSystem Console, and the **Instances** screen in the CloudSystem Portal to manage and monitor instances deployed from CloudSystem Enterprise.

Prerequisites

- Minimum required privileges: Infrastructure Administrator.
- Identify and record the names of instances created in Enterprise. If you reinstall Enterprise at a future time, you will need this information to deploy the instances from Enterprise.

Procedure 77 Uninstalling CloudSystem Enterprise

1. From the main menu, select **Enterprise**.
2. Click **Actions→Uninstall CloudSystem Enterprise**.

   The **Uninstall CloudSystem Enterprise** screen is displayed.

3. Review the instructions, then click **Yes, uninstall**.

   To exit the action without uninstalling Enterprise, click **Cancel**.

4. Verify that the Enterprise appliance was removed. The name of the virtual machine where the Enterprise appliance is running is automatically designated based on the management hypervisor hostname (ESX or KVM). For example, if the management hypervisor host name is **my-host-name.example.com** then the Enterprise appliance name is **my-host-name**.
   - If previously installed on ESX, confirm the Enterprise appliance is no longer listed in vCenter Server in the cluster.
   - If previously installed on KVM, log into the management hypervisor and enter the command

     ```
     virsh list --all
     ```

     Enterprise will not be listed along with the base appliance, SDN controller and network node appliances.

Enterprise appliance settings

Enterprise appliance settings display on the Enterprise overview screen after Enterprise is installed.

Viewing Enterprise appliance settings

The CloudSystem Enterprise pane on the **Enterprise** screen displays information about the Enterprise appliance:

- Enterprise appliance host name
- IP address of the Enterprise appliance
- Model of the Enterprise appliance

- Current date and time
- Version and date of the Enterprise appliance software

25 Cloud service provisioning and deployment in Enterprise

Service provisioning and deployment in CloudSystem Enterprise is done through the Cloud Service Management Console. This chapter gives you an introductory set of processes to get started using this console. Consult HP CSA documentation at Enterprise Information Library for details.

Using HP CSA to deploy virtual machine instances to the cloud

After Enterprise is installed and configuration in HP Cloud Service Automation is complete, you can use HP CSA to create designs and the Marketplace Portal to launch instances. These instances can be managed from the CloudSystem Console and the Cloud Service Management Console.

See also Logging in and changing the default HP CSA and Marketplace Portal password (page 128).

For more information about the tasks in the following table, see:

- HP CSA documentation at Enterprise Information Library

☑	Task
	1. Create a design in HP CSA The design defines the instance characteristics and network details. When a design is saved, it can be published and made into an offering that other users can purchase and provision from the Marketplace Portal.
	2. Deploy an offering In the Marketplace Portal, select an offering and submit the request. View the Marketplace Dashboard to verify that the instance was created.
	3. Verify the instance In the Foundation CloudSystem Portal, verify that the instance is listed on the **Instances** screen with an active status.

Using HP CSA to create a design and deploy an offering

When the Cloud OS provider is configured in HP CSA, you can create a design, convert a design to an offering and deploy the offering.

IMPORTANT: If you have added additional providers, such as HP Server Automation, HP Matrix Operating Environment, or VMware vCenter Server, then make sure the providers are added to an environment, and the environment is associated with each catalog where you plan to publish offerings.

See "Configuring additional providers for CloudSystem Enterprise" in the *HP CloudSystem 8.0 Installation and Configuration Guide* at Enterprise Information Library.

Prerequisites

- Enterprise was successfully installed from CloudSystem Foundation.
- A Provider network is created in CloudSystem Foundation.

  To find help on creating these networks, log in to CloudSystem Foundation, select **Provider Networks** from the main menu, then click the ? icon in the top right corner of the screen and select "Help on this page".

- An image is created in CloudSystem Foundation.

  To find help on creating images, log in to CloudSystem Foundation, select **Images** from the main menu, then click the ? icon in the top right corner of the screen and select "Help on this page".

- A key pair is created in the CloudSystem Portal.

  See Create a key pair (page 119).

Set up a template

Procedure 78 Setting up a template

1. Log in to the CloudSystem Console.
2. Navigate to **Enterprise** on the main menu.
3. In the Tools pane, click Cloud Service Management Console.

   This link opens the HP CSA console.
4. Log in with the default user name (admin) and password (cloud).

   See Logging in and changing the default HP CSA and Marketplace Portal password (page 128).
5. Select **Designs→Topology**.
6. Click **Create** at the bottom of the screen.

   The **Create New Design** window opens.
7. Enter the General details for the new template:
   a. Enter a name for the template.
   b. Enter an optional description.
   c. Click **Next**.
   d. Select a provider and resource pool.
   e. Click **Next**.
   f. If you want to add category tags, then click the **Manage Tags** link at the bottom of the window and add the tags.

      Click **Next** when finished.
   g. Select an image to associate with the design.
   h. Click **Finish**.

      A blank Editor opens for the design.

      For assistance, click the ? icon in the top right corner of the screen.

Create a server group

Procedure 79 Creating a server group

Create the server group in the blank Editor pane of the new design.

1. Left-click a gray square shadow in the white space to reveal the **Create** actions.
2. Select the **server group** option.
3. Find the server details along the right side of the window. Enter the following details:
   a. A name for the server group
   b. An Instance name prefix.

   IMPORTANT: Use `enterprise-` as the prefix so that you can identify instances deployed from Enterprise when you are viewing the Instances screen in Foundation.

   c. Enter the minimum and maximum number of instances.

4. Select an image used to create the server group.
5. Select a flavor, which describes the machine configuration size (amount of memory, number of CPUs, and ephemeral disk space available) used to create new VMs.
6. Enter a pre-create callout, if needed. Specify the UUID of an Operations Orchestration flow that is to be called before the object is created. A flow can read and write provider property values during service provisioning.
7. Enter a post-create callout, if needed. Specify the UUID of an Operations Orchestration flow that is to be called after the object is created.
8. Click **Save** in the bottom left corner.

Connect a network to the server group

Procedure 80 Connecting a network to server group

1. Click a gray square shadow in the white space to reveal the **Create** actions.
2. Select the **network segment** option.
3. Find the network details along the right side of the screen. Enter the following details:
   a. Enter a name for the network segment.
   b. Select a type.
   c. Select a network. Networks created in Foundation display in the Network drop down list. Provider networks are created in the CloudSystem Console. Private networks are created in the CloudSystem Portal.

      See Network configuration (page 73).
   d. Select a subnet.
4. Click **Save**.
5. Click one of the open circles to the side of the network segment and drag it to the server you created.

   A gray connection appears between the network and the server.
6. Enter the Network Interface details. Make sure the line connecting the network and server is highlighted blue to access the interface details on the right side of the screen.
   a. Select a security group. Security groups are created in the CloudSystem Portal.

      See Create a security group (page 118).
   b. Choose whether or not to assign floating IP addresses.
7. Click **Publish**.

Create an offering

Procedure 81 Creating an offering and associating it to a Global Catalog

1. Navigate back to the HP CSA Dashboard and select **Offerings**.
2. Select **Create**.

   The **Create Offering** window opens.
3. Select the design you created and enter a display name, then click **Create**.
4. Click **Publish**.

   The **Publish Service Offering** window displays.
5. Select the **Global Shared Catalog**.
6. In the Category drop down list, select **Simple System**.
7. If needed, select an approval policy.
8. Click **Publish**.

Deploy an offering

Procedure 82 Deploying an offering

1. From the CloudSystem Console main menu, select Enterprise. In the Tools pane, click the Marketplace Portal link.
2. Log in to Marketplace Portal.

   See Logging in and changing the default HP CSA and Marketplace Portal password (page 128).
3. Select **Browse Catalog** and click the new offering that you created.
4. Select a keypair from the drop down list. This will give you permission to log into the instance in Foundation.
5. Verify the details of the offering, and if correct, click **Checkout**.
6. From the Service Checkout screen, complete the required information and then click **Submit Request**.
7. Use the **My Services** option on the Marketplace Dashboard to view your subscription and verify that it comes online.
8. Log in to the Foundation CloudSystem Portal.

   To access the CloudSystem Portal, open a new browser tab and copy the CloudSystem Foundation address, then modify it by appending `/portal`. For example: `https://192.0.2.2/portal`.
9. Select the **Projects** tab and click **Instances** on the left menu.
10. Verify that the new instance displays on the Instances screen.

    You should also see the instance on the **Instances** screen in the CloudSystem Console.

Part VI Troubleshooting reference

26 Use activities and alerts to troubleshoot errors

Basic troubleshooting techniques

HP CloudSystem has a variety of troubleshooting tools you can use to resolve issues. By following a combined approach of examining screens and logs, you can obtain a history of activity and the errors encountered.

- The Activity screen displays a log of all changes made on the appliance, whether user-initiated or appliance-initiated. It is similar to an audit log, but with finer detail and it is easier to access from the UI.

  The **Activity** screen also provides a log of health alerts and status notifications.
- Download an audit log to help you understand what security relevant actions took place on the system.
- Create a support dump file to gather logs and other information required for debugging into an encrypted, compressed file that you can send to your authorized support representative for analysis.

Recommendation	Details
Look for a message	**About syntax errors:** • The user interface checks for syntax when you enter a value. If you make a syntax error, an instructional message appears next to the entry. The user interface or command line continues to display messages until you enter the correct value. **About network setup errors:** • Before applying them, the appliance verifies key network parameters like the IP address and the fully qualified domain name (FQDN), to ensure that they have the proper format. • After network settings are applied, the appliance performs additional validation, such as reachability checks and host name to IP lookup. If a parameter is incorrect, the appliance generates an alert that describes validation errors for the Network Interface Card (NIC), and the connection between the browser and the appliance can be lost.
Examine the Activity screen	**To find a message for an activity:** 1. Locate recent activities with a severity of **Critical**, **Warning**, or **Unknown**. 2. Read the message for problem identification and potential solutions. 3. Expand the activity to add notes to the activity details.
Examine the appliance virtual machine	**When VM host is down or nonresponsive:** 1. From the local computer, use the `ping` command to determine if you can reach the appliance. • If the `ping` command is successful, determine that the browser settings, especially the proxy server, are correct. Consider bypassing the proxy server. • If the `ping` command did not reach the appliance, ensure that the appliance is connected to the network. 2. Log onto hypervisor to verify that the hypervisor is running. 3. Verify that the virtual guest for the appliance is operational. 4. Ensure that the VM host configuration is valid. Verify the accuracy of the IP address and other network parameters for the VM host.

Recommendation	Details
	5. From the management console, ensure that the appliance network settings are accurate. For information, see Change the appliance host name, IP address, subnet mask, or gateway address (page 46). 6. Examine the hypervisor performance data. If the appliance is running at 100% utilization, restart the hypervisor.

Enable console access	**About console access:**
	• Use the following `csadmin` console-users CLI commands to enable console access and set the password. After running the command, you can locate logs for additional troubleshooting information. The *`VM_name`* is the virtual machine where you want to execute the command. The `csadmin` console-users commands are supported on the Foundation base appliance, the Enterprise appliance, and the Proxy appliances.
	To enable console access:
	1. Open the CLI.
	2. Enter the command:
	`csadmin console-users enable --vm-name VM_name`
	To set the password console access:
	• Open the CLI.
	• Enter the command:
	`csadmin console-users set-password --password CAPasswd --vm-name VM_name`
	Where *`CAPasswd`* is the password for the Cloud Administrator.

Alerts do not behave as expected

Symptom	Possible cause and recommendation
Alerts are not generated	**Appliance out of compliance** The peak number of virtual machines exceeds the licenses. 1. Add a license key to the appliance (page 65). 2. Apply the licenses to unlicensed virtual machines.
Alert is locked and cannot be cleared	**Locked alert was created by a resource** 1. Expand the alert and follow the recommended action described in **Resolution**. 2. If you need more information, expand the **Event details** and see the details for **correctiveAction**. 3. When the resource detects a change, it will automatically change the alert status to `Cleared`.
Alerts are not visible in the UI	**Improper permission** 1. If possible, log in as a privileged user. Otherwise, request that the Infrastructure administrator change your role so that you can see alerts for the physical resource type. 2. View the **Activity** screen.
Alert status is other than Critical, Warning, OK, or Unknown	**Blank or unexpected status reported for the alert** 1. Clear the alert. 2. Restore the alert.
Alert state is other than Active, Locked, or Cleared	**Resource reported an unexpected alert state for an underlying problem** 1. Expand the alert and follow the recommended action described in **Resolution**. 2. If you need more information, expand the **Event details** and see the details for **correctiveAction**. 3. When the resource detects a change, it will automatically change the alert state to `Cleared`.

27 Troubleshoot the CloudSystem appliances

Troubleshooting the Foundation base appliance

You cannot log in

Symptom	Possible cause and recommendation
There is no login screen.	**Appliance not yet started or browser not behaving correctly** 1. Wait for the appliance to start completely. 2. Refresh your browser and try again. 3. Open a new browser and try again. 4. As Infrastructure administrator, restart the appliance and try again.
There is a login screen, but the appliance rejects your login.	**Invalid authentication** 1. Retype your login name and password in case you made an error. 2. Verify your login name and your group and role settings with the Infrastructure administrator. If the appliance was reset to its original factory settings, the Infrastructure administrator might need to reinstate you. 3. As Infrastructure administrator, restart the appliance and try again.

First-time setup

Symptoms	Possible causes and recommendations
Appliance cannot access network	**Appliance network settings are not properly configured** Minimum required privileges: Infrastructure administrator 1. Access the appliance console. 2. Examine the alerts on the **Activity** screen to help diagnose the problem. 3. On the **Settings** screen, verify that the following entries are correct: • Host name (if DNS is used, ensure that the appliance host name is a fully qualified domain name) • IP address • Subnet mask • Gateway address 4. For manual DNS assignment, verify that there are no errors in the IP addresses you entered for the primary and secondary DNS servers.

Symptoms	Possible causes and recommendations
	5. Verify that your local router is working. 6. Verify that the network is up and running.
Appliance is configured correctly but cannot access network	**External difficulties** 1. Verify that your local router is working. 2. Verify that the network is up and running.

Appliance cannot access the network

Symptom	Possible cause and recommendation
Appliance cannot access the network	**Appliance network not properly configured** Minimum required privileges: Infrastructure administrator 1. Verify that the IP address assignment is correct. 2. Verify that the DNS IP address is correct. 3. Verify that the DNS server is running.

Time differences among CloudSystem appliances and management hosts cause unpredictable behavior

Symptom	Possible cause and recommendation

• **In Foundation, you see unpredictable system behavior**
• **In Enterprise when you try to create a design, images and flavors are not displayed and you see** `Connection error, status code 500`
	Time is not synchronized on the Foundation base appliance, Enterprise appliance, vProxy appliance, Matrix OE CMS, and the Foundation and Enterprise management hosts
	When CloudSystem is installed on an **ESX** management hypervisor:
	1. Ensure that the **VM hosts** running the Foundation base appliance and Enterprise appliance are synchronized with the same set of NTP servers.
	Do not change the time settings of the associated CloudSystem Foundation appliances using the vCenter Server.
	2. Configure the Foundation appliance to synchronize with these NTP servers.
	a. On the CloudSystem Console **Settings** screen, click the Edit icon in the Appliance panel. In the Time and Language settings section, change the setting to **Synchronize with time server**.
	b. Enter the IP address of the external NTP servers.
	3. Configure the Enterprise appliance to synchronize with these NTP servers.
	Access the CloudSystem Enterprise appliance console from the management hypervisor console.
	For instructions, see Supported console operations on the CloudSystem appliances (page 199).
	a. Edit the NTP configuration file to add the NTP server entries.
	`sudo vi/etc/ntp.conf`
	b. Restart the NTP service.
	`sudo service ntpd restart`
	4. Restart the Enterprise appliance using the ESX hypervisor management software.
	When CloudSystem is installed on an **KVM** management hypervisor:
	1. Ensure that the **VM hosts** running the Foundation base appliance and Enterprise appliance are synchronized with the same set of NTP servers.
	2. On the CloudSystem Console **Settings** screen, click the Edit icon in the Appliance panel. In the Time and Language settings section, ensure that the default setting of **Synchronize with VM host** is checked.
	3. Restart the Enterprise appliance using the KVM hypervisor management software.

Reboot appliance after serious error

Symptom	Possible cause and recommendation

You see **The appliance has encountered a serious error**	**Rebooting the appliance may solve the problem**
	1. Log in to the management KVM host on which the Foundation appliance is running and enter the command:
	`virsh reboot hypervisor-name`
	2. Open the CloudSystem Console in your browser and wait for a login screen, then log in.
	3. If a login screen does not appear, enter the following commands on the management hypervisor
	`virsh shutdown hypervisor-name`
	`virsh start hypervisor-name`
	4. Consider creating a support dump and sending it to HP to help diagnose the problem that occurred and to help improve the product.
	See Create a support dump file (page 39).

Cannot restart or shut down appliance

Symptom	Possible cause and recommendation
The appliance did not shut down	**Internal server error** Minimum required privileges: Infrastructure administrator 1. Retry the shutdown action. 2. If the problem persists, create a support dump. 3. Contact your authorized support representative and provide them with the support dump. For information on contacting HP, see How to contact HP (page 41).
Cannot restart the appliance after a shutdown	**Internal server error** Minimum required privileges: Infrastructure administrator 1. Retry the restart action. 2. If the problem persists, create a support dump. For information, see Create a support dump file (page 39). 3. Contact your authorized support representative and provide them with the support dump. For information on contacting HP, see How to contact HP (page 41).

Generated host name of the base appliance is sometimes visible

Symptom	Possible cause and recommendation
The host name has the prefix "ci-" followed by the MAC address of the a virtual NIC in the base appliance. You may see this name in the output of commands such as `nova service-list`	**The OpenStack CLI shows an incorrect host name for the Foundation base appliance when it is hosted on a KVM hypervisor.** • You can ignore this host name if it appears.

Audit log

Symptom	Possible cause and recommendation
Could not download audit log	**Improper authorization** Minimum required privileges: Infrastructure administrator 1. Only the Infrastructure administrator can download the audit log. Log in and then download the audit log.
Downloaded audit log is missing	**Audit log was deleted** Minimum required privileges: Infrastructure administrator 1. Restart the appliance to create a new audit log and resume logging.
Entries are not logged	**Audit log was edited** Minimum required privileges: Infrastructure administrator 1. Restart the appliance to create a new audit log and resume logging.
Audit log is absent	**Audit log was deleted** Minimum required privileges: Infrastructure administrator 1. Restart the appliance to create a new audit log and resume logging.

Cannot create a support dump file

Symptom	Possible cause and recommendation
Support dump file not created	**Insufficient time** Minimum required privileges: Infrastructure administrator 1. Wait. Creating a support dump file can take several minutes. If the log files are large or if the system is extensive, creating a support dump file can take even longer. 2. Retry the create support dump action. **Insufficient disk space** Minimum required privileges: Infrastructure administrator 1. Ensure that the appliance has more than 300 MB to accommodate the support dump file. 2. Retry the create support dump action.
Support dump file not saved	**Insufficient disk space** Minimum required privileges: Infrastructure administrator 1. Ensure that the local computer has more than 300 MB to accommodate the support dump file. 2. Retry the create support dump action.

Licensing

Symptom	Possible cause and recommendation
Could not add license key	**License key is blank, incorrect, or invalid** 1. Verify the license key you entered. 2. Provide proper values and make sure that the license key format is valid. 3. Try again. 4. If the problem persists, contact your authorized support representative. **License is already in use** 1. Acquire a different license key. 2. Try again with the new license key.

Symptom	Possible cause and recommendation
	License key has expired 1. Acquire a valid, current license key. 2. Try again with the new license key.
Could not view license details	**No license is assigned to the appliance** 1. Assign the license. 2. Retry the operation. **Filter entry is blank or incorrect** 1. Correct the filter criteria. 2. Retry the operation.

Troubleshooting appliance update

- Version error prevents appliance update (page 145)

Version error prevents appliance update

Symptom	Possible cause and recommendation
You see `Same version is already installed`	**The version you are attempting to install is already installed** 1. Go to the **Settings→Actions** drop down list and select **Update Foundation appliances**. 2. Follow the Update Foundation appliances (page 48) instructions.
You see `A higher version is already installed`	**You are attempting to install a version of the update kit that is older than the currently installed version** 1. Go to the **Settings→Actions** drop down list and select **Update Foundation appliances**. 2. Follow the Update Foundation appliances (page 48) instructions.

Error occurs during update process

Symptom	Possible cause and recommendation
You see `There was an unexpected problem moving the file to the system`	**A file with an incorrect format was selected on the update appliance screen** 1. Go to the **Settings→Actions** drop down list and select **Update Foundation appliances**. 2. Select the correct file format (extension.bin). 3. Follow the Update Foundation appliances (page 48) instructions.
You see `The appliance is about to restart. Upgrade failed, reverting snapshots`	**A critical error occurred and the appliance reverted to the current version** 1. Wait for the system to recover. All file system data that was saved before the upgrade process started will be recovered. 2. Retry the update process using the Update Foundation appliances (page 48) instructions.

Troubleshooting users and groups

NOTE: For information about configuring users and groups, see Manage users and groups (page 52) and Configuring CloudSystem to use Active Directory or OpenLDAP directory authentication (page 55).

Cannot log in to the CloudSystem Portal

Symptom	Possible cause and recommendation
You cannot log in to the CloudSystem Portal	**The infrastructure administrator was added in the CloudSystem Console but has not logged in to the CloudSystem Console** 1. Log in to the CloudSystem Console at least once. 2. Log in to the CloudSystem Portal. **You enabled directory service authentication when users exist in the CloudSystem Portal** Users previously added in the CloudSystem Portal cannot log in. As a best practice, do not add users in the CloudSystem Portal if you plan to enable directory service authentication. 1. Log in to the CloudSystem Portal as an administrator user and assign the users in the group as members of an existing project. 2. If you set a password for these users, inform the users of the changed password. **A directory group contains the same user name as another local user created in the CloudSystem Console** When the new local user logs in to the on CloudSystem Console, the existing directory group user cannot log in the CloudSystem Portal and is no longer assigned to a project. • Delete the duplicate user from CloudSystem Console and create another user with a different name and assign the user to a project, or • Disable local logins. (HP does not recommended this action because with local logins disabled, you cannot log in to the CloudSystem Console when the directory server is unavailable.) **You changed an infrastructure administrator user's role from Full to Read only or Specialized in the CloudSystem Console** This change removes the administrator role from the user in the Administrator project in the CloudSystem Portal. After the change takes effect, the user can no longer log in to the Portal if the user is assigned only to the Administrator project. (The user can log in to the Portal if the user is assigned to a project other than the Administrator project.) 1. Log in to the CloudSystem Portal using another administrator account, and assign the user to the administrator or member role in an existing (non-Administrator) project. 2. Ask the user to log in to the Console or the Portal to complete the change.

Symptom	Possible cause and recommendation
	You changed a group's role from Full to Read only or Specialized in the CloudSystem Console 1. Log in to the CloudSystem Portal as an administrator user and assign the users in the group as members of an existing project, or 2. Change the role assignment of the group in the CloudSystem Console to Full.

Cannot perform actions in the CloudSystem Console that affect resources in the CloudSystem Portal

Symptom	Possible cause and recommendation
You see an error when you try to perform actions in the Console that affect resources in the Portal, for example, deleting instances, creating images, adding provider or private networks, and creating volume types	**An Infrastructure administrator or other local user was created in the CloudSystem Console and the user already exists in the CloudSystem Portal** • Delete the user from the CloudSystem Portal and ask the user to log in to the CloudSystem Console. **An Infrastructure administrator logged in to the CloudSystem Console and selected a directory service when Local or another directory is the default directory** • Set the directory as the default service to use for authentication. On the CloudSystem Console **Settings** screen, click the Edit icon in the Security pane. Under Directories, select an authentication directory service, then click OK. As a best practice, do not configure more than one directory service. **A directory group contains a user with the "administrator" user name or the group contains the same name as another local user created in the CloudSystem Console** • Delete the duplicate user from CloudSystem Console and create another user a with different name, or • Disable local logins. (HP does not recommended this action because with local logins disabled, you cannot log in to the CloudSystem Console when the directory server is unavailable.) **Local authentication database and directory service database has a different password for the same user** If an infrastructure administrator logs into the CloudSystem Console using local authentication and directory service authentication is enabled, then both the local and directory database must be configured to accept the same password. • Ensure that the configured local and directory authentication services for the CloudSystem Console and CloudSystem Portal are configured to accept the same password for the identical infrastructure administrator login name.

Cannot add, delete, or modify users in the CloudSystem Portal

Symptom	Possible cause and recommendation
You see `Error: Unauthorized: Unable to create user` or `Error: An error occurred. Please try again later` **when you try to add, edit, or delete a user in the CloudSystem Portal**	**OpenLDAP or Active Directory is configured to authenticate users** Directory group users cannot be edited or deleted in the CloudSystem Portal when directory service authentication is enabled. • Use enterprise directory software (OpenLDAP or Active Directory) to manage user accounts. **Users were added in the CloudSystem Console** Local users added in the CloudSystem Console cannot be edited or deleted in the CloudSystem Portal. • Use the CloudSystem Console to manage user accounts created in the CloudSystem Console.

Users with names containing special characters cannot be assigned to projects

Symptom	Possible cause and recommendation
• When you attempt to assign the user to a project, you see `Success: Modified project <project-name>` • The user is not actually assigned to the project, and if you attempt to revoke the user from the project, the user is not listed under Project Members	**The user name contains special characters** • Use the OpenStack Keystone CLI to assign an OpenLDAP or Active Directory to a project when the user name contains special characters.

Changing the default directory from two sessions of the CloudSystem Console at the same time does not update keystone.conf correctly

Symptom	Possible cause and recommendation
You cannot restart the OpenStack Keystone service and the Foundation base appliance reboots	**Administrators accessing two or more sessions of the CloudSystem Console changed the default directory at the same time** 1. Restore the appliance snapshot (backup) to restore the `keystone.conf` file. 2. Restart the Keystone service.

Troubleshooting security settings

Directory service not available

Symptom	Possible cause and recommendation
Cannot connect to the directory service	**Directory service server is down** 1. Locally run the `ping` command on the directory server IP address or host name to determine if it is online. 2. Verify that the appliance network is operating correctly. 3. Contact the directory service administrator to determine if the server is down. **Inaccurate settings in the Add Directory screen** 1. Verify that the name of the directory service is unique and entered correctly. Duplicate names are not accepted. 2. Verify that the **Directory type** is correct. 3. Ensure that the **Search context** fields are correct. Verify that the group is configured in the directory service. 4. Verify that the credentials of the authentication directory service administrator are correct. 5. Ensure that the role assigned to the group is correct.

Cannot add directory service

Symptom	Possible cause and recommendation
Connectivity	**Lost connection with directory service host** 1. Verify that the settings for the directory service host are accurate. 2. Locally run the `ping` command on the directory server's IP address or host name to determine if it is on-line. 3. Verify that the port for LDAP communication with the directory service is correct. 4. Verify that the port you are using for communication is not blocked by any firewalls. 5. Verify that the appliance network is operating correctly. 6. Determine that the appliance virtual machine is functioning properly and that there are enough resources.
Cannot log in	**Inaccurate credentials** 1. Verify the login name and password are accurate. 2. Verify the search context information is accurate; you might be trying to access a different account or group. 3. Re-acquire and install the directory service host certificate. 4. Contact the directory service provider to ensure that the credentials are accurate.

Cannot add server for a directory service

Symptom	Possible cause and recommendation
Connectivity	**Lost connection with directory service host** 1. 2. Verify that the correct port is used for the directory service. 3. Verify that the port you are using for communication is not blocked by any firewalls. 4. Locally run the `ping` command on the directory service host's IP address or host name to determine if it is on-line. 5. Verify that the appliance network is operating correctly. 6. If the appliance is hosted on a virtual machine, determine that it is functioning properly and there are enough resources.
Cannot log in	**Inaccurate credentials** 1. Verify that the login name and password are accurate. 2. Reacquire and install the directory service host certificate. 3. Contact the directory service provider to ensure that the credentials are accurate. **Inaccurate settings in the Add Directory screen** 1. Verify that the name of the directory service is unique and entered correctly. Duplicate names are not accepted. 2. Verify that the **Directory type** is correct. 3. Ensure that the **Search context** fields are correct. Verify that the group is configured in the directory service. 4. Verify that the credentials of the authentication directory service administrator are correct.

Cannot add directory group

Symptom	Possible cause and recommendation
Cannot log in	**Lost connection with directory service host** 1. Verify that the settings for the directory service host are accurate. 2. Verify that the correct port is used for the directory service. 3. Verify that the port you are using for communication is not blocked by any firewalls. 4. Locally run the `ping` command on the directory service host IP address or host name to determine if it is online. 5. Verify that the appliance network is operating correctly. 6. If the appliance is hosted on a virtual machine, determine that the virtual machine is functioning properly and enough resources are allocated to it. **Inaccurate credentials** 1. Verify that the login name and password are accurate. 2. Reacquire and install the directory service host certificate. 3. Contact the directory service provider to ensure that the credentials are accurate.
Cannot find group in the directory service	**Group not configured in the directory service** 1. Verify the name of the group. 2. Contact the directory service administrator to verify that the group account is configured in the directory service. 3. Verify that the group is within four hierarchical levels from the group specified by the DN. For more information, see About directory service authentication (page 53).

No error message is displayed after adding an invalid public key

Symptom	Possible cause and recommendation
The invalid public key you entered is not saved and and an error message is not displayed	**You entered an invalid public key when you previously entered a valid key** • Enter the valid public key and make sure to copy the key exactly, without adding newlines or whitespace. The key is viewable from the hp.com link on the **Settings→Edit Security** screen.

Unable to create a security group in CloudSystem Portal

Symptom	Possible cause and recommendation
On creating a Security Group you see the following error: `Unable to create security group.`	**The project quota has been reached.** 1. From the **Project** tab, select **Manage Compute→Overview**. The **Limit Summary** screen is displayed. 2. Check that the **Security Groups** have not reached the limits. 3. If the **Security Groups** have reached the limits, select **Manage Compute→Access & Security**. 4. Delete a security group that is no longer needed, and then retry creating the security group. **NOTE:** Also you can try reusing an existing security group rather than create a new one, or ask the administrator to increase the quota.

Unauthorized CloudSystem Portal users can see project resources

Symptom	Possible cause and recommendation
A user in the CloudSystem Portal can view and change resources in projects for which they are not authorized	**Default directory was changed and the same user name in both the old and new directory identifies different individuals** For example, consider the scenario where `steve.users.lab.example1.com` is assigned to Project A. If you change the default directory from "Lab" to "Marketing" and the new directory includes `steve.users.marketing.example1.com`, then both users named "Steve" have access to Project A. This is a security issue. 1. Revoke one of the duplicate user names from Project A in the OpenStack Identity (Keystone) database. See About directory service authentication (page 53).

Troubleshooting the CloudSystem Portal appliance

You cannot log in to the CloudSystem Portal

Symptom	Possible cause and recommendation
You are a newly designated Infrastructure administrator and you see the error `Invalid user name or password`	**The credentials that allow an Infrastructure administrator to log into the CloudSystem Portal are not created** 1. Log in to the CloudSystem Console. 2. Log in to the CloudSystem Portal. Credentials are generated when the administrator logs into the CloudSystem Console.
The error `You don't have permissions to access: /portal/admin/info/` is displayed	**Possible communication error with OpenStack Identity (Keystone) service** 1. Exit the browser and restart it. 2. Log in to the CloudSystem Portal again.

You are logged out of the CloudSystem Console while using the CloudSystem Portal

Symptom	Possible cause and recommendation
The system logs you out of the CloudSystem Console while you are using the CloudSystem Portal to launch an instance console	**Conflict between console sessions** 1. Log in to the CloudSystem Console again.

Resource information in the CloudSystem Portal does not always match the CloudSystem Console

Symptom	Possible cause and recommendation
• In the CloudSystem Portal, you see the number of active instances for a specific time period (by default, the current month). In the CloudSystem Console, you see the number of active instances at the current point in time. • In the CloudSystem Portal, you see the number of active instances as instances in all states (including Shutoff and Suspended). In the CloudSystem Console, active instances are instances only in the Active state. • In the CloudSystem Portal, you see the uptime and amount of memory used by instances in all states. In the CloudSystem Console, the amount of memory used is shown for instances in the Active state. • In the CloudSystem Portal, the status of an instance that has changed to "Rescue" is not updated in the CloudSystem Console. The status in the Console remains "Active." • In the CloudSystem Portal, when adding a new flavor, you must specify additional flavor details that are not required in the CloudSystem Console. When viewing flavors, the extra flavor details are not visible in the CloudSystem Console, and any fields that were not required when the flavor was created in the CloudSystem Console are filled with a value of "0" in the CloudSystem Portal.	**Information in the CloudSystem Portal and CloudSystem Console is calculated and displayed in different ways** • Note the different methods of displaying the information.

Virtual machine console cannot be accessed

Symptom	Possible cause and recommendation
When opening the virtual machine console in the CloudSystem Portal, the CloudSystem Portal does not connect to the virtual machine	**Port not opened in the compute node security profile** 1. Log in to vCenter Server. 2. Select the compute hypervisor and click the **Configuration** tab. 3. Click **Security Profile** in the left menu. 4. Open Firewall Properties and add the option **VM serial port connected over network**.

Volumes search filter always returns the last created volume

Symptom	Possible cause and recommendation
The last volume created is always returned when you search for a volume in the CloudSystem Portal	**The CloudSystem Portal does not update the search index correctly** • After adding, deleting, or updating a volume, refresh the **Volumes** screen, then use the search filter.

Volumes with duplicate names can be created

Symptom	Possible cause and recommendation
When you create more than one volume with the same name, no error is displayed, and the volumes are successfully created	**The CloudSystem Portal identifies volumes by ID instead of name** • Expand the volume detail to see the volume ID, which is not duplicated. • As a best practice when creating a volume, specify a unique name for each volume.

28 Troubleshoot resource configuration

Troubleshooting networks

Cloud Management Network configuration fails due to a timeout occurring while creating associated virtual machines

Symptom	Possible cause and recommendation
You see the message `Unable to setup Cloud Management network: Timed out waiting for ...` when you save the Cloud Management Network configuration on the Settings→Edit Cloud Networking screen in the CloudSystem Console	**Occasionally there is not enough time for the Foundation appliance to automatically create the Software Defined Network (SDN) controller and the three network node appliances within the time allocated by various timeout values** 1. Retry the action by re-entering the Cloud Management Network settings and clicking **OK** again. When you retry the configuration, the virtual machines are removed and recreated. It is often faster to create the virtual machines the second time because the images used to create the virtual machines may not need to be copied. 2. If retrying right away does not work, wait until the the hypervisor, storage system, and networks are less busy, then retry again. 3. Ensure that your hardware meets the requirements specified in the *HP CloudSystem 8.0 Installation and Configuration Guide*.

Software Defined Networking (SDN) issues

Symptom	Possible cause and recommendation
You cannot restart SDN agents	**SDN agents do not join the controller after restarting the network node when the Cloud Management Network is unavailable** When the Cloud Management Network is unavailable, all communication among the CloudSystem Foundation associated VMs and compute nodes is disrupted. If you try to restart

Symptom	Possible cause and recommendation
	the SDN agents on the compute node and network node while the network is down, SDN agents cannot recover when the network is online again. 1. When the Cloud Management Network is back online, restart the SDN agents again, or reboot the compute node and network node.
After a power interruption on the management cluster or hypervisor, you lose Foundation SDN appliance data	**The OpenStack Neutron database on the SDN appliance may be corrupted** 1. Restore the SDN database. See the *HP CloudSystem 8.0: Recommended backup and restore procedures* white paper at Enterprise Information Library.

Cannot create a private network

Symptom	Possible cause and recommendation
You do not see information about a private network that you want to create for a project in the CloudSystem Portal or the CloudSystem Console	**The private network creation process is not complete** Complete the steps to create a private network in the following order. 1. In the CloudSystem Console, add VLAN IDs to the pool of VLANs available for Private Network assignments. See Add VLAN IDs (page 76). 2. Verify that the new VLAN IDs are listed on the **Private Networks** overview screen. 3. In the CloudSystem Portal, create a network. (**Admin→Networks→+ Create Network→Create Network**) The OpenStack Networking service assigns to the project a VLAN ID from the VLAN IDs you allocated in the console. 4. Verify that the new network is listed on the **Networks** overview screen. See also About Private Networks (page 76).

Cannot delete a private network in the CloudSystem Portal

Symptom	Possible cause and recommendation
You see a `Failed to delete` message when you try to delete a private network in the CloudSystem Portal	**One or more instances is using the private network** 1. On the CloudSystem Portal **Instances** screen, review the **IP Address** listings to determine which instance(s) are assigned the same IP address as the private network that you want to delete.. 2. Delete each instance that is using the private network. See Delete instance (page 109). 3. Retry deleting the private network.

Cannot add a router with a port using the CloudSystem Portal or the OpenStack Neutron CLI

Symptom	Possible cause and recommendation

You see an `Incompatible type` error when you specify an IP address for a private or provider network router interface	**The network port settings are incorrect**
	1. Use one of the following methods to create a network with the correct port settings.
	• Using the CloudSystem Portal:
	a. Create a network.
	b. Create a subnet under the network.
	c. Create a router and note the `routerId`, which will be used as the `device-id` when you create a port.
	d. Create a port and specify the `device-id` from step 3 and specify the device owner as `network:router_interface`.
	e. Verify that the router-interface was created when you see the "Success: Port was successfully created" message.
	• Using the OpenStack Neutron CLI:
	a. Create a port with the `device_owner` attribute set to `network:router_interface`, then enter `router-interface-add <router> port=<port-id>`.
	For example:
	`# neutron port-create -name port1 --device_owner network:router_interface -fixed-ip ip_address=IP_ADDR`
	`# neutron router-interface-add <router> port=port1`

External Network information is not listed on the CloudSystem Portal

Symptom	Possible cause and recommendation
You cannot see the External Network listed on the Networks screen in the CloudSystem Portal	**The External Network that was automatically created during CloudSystem Foundation installation has been deleted** 1. On a Windows or Linux workstation where the OpenStack CLI package for CloudSystem is installed, log on to the management hypervisor on the base appliance. 2. Recreate the External Network by entering this command on the command line: `neutron --insecure net-create 'External Network' --provider:physical_network provider --provider:network_type vlan --provider:segmentation_id 0 --router:external=True` 3. In the CloudSystem Portal, verify that the External Network is listed on the **Networks** screen with a VLAN ID as its "Subnets Associated" component.
You cannot see a VLAN ID listed for the External Network on the Networks screen in the CloudSystem Portal	**The External Network has been recreated on the CloudSystem Portal instead of from the management hypervisor command line** An External Network recreated in the CloudSystem Portal will not have a VLAN ID associated with it. 1. In the CloudSystem Portal, delete the External Network that does not have a VLAN ID. (**Admin**→**Networks**→**Actions**→**Delete Network**) 2. Verify that there is no External Network listed on the **Networks** screen. 3. On a Windows or Linux workstation where the OpenStack CLI package for CloudSystem is installed,log on to the management hypervisor on the base appliance. 4. Create a new External Network by entering this command on the command line: `neutron --insecure net-create 'External Network' --provider:physical_network provider --provider:network_type vlan --provider:segmentation_id 0 --router:external=True` 5. In the CloudSystem Portal, verify that the new External Network is listed on the **Networks** screen with a VLAN ID as its "Subnets Associated" component.

OpenStack Nova command errors

Symptom	Possible cause and recommendation
After you execute the `nova interface-attach <server>` command, you see a `Failed to attach interface` error message	**You are not specifying an `id` value** If you run the `nova interface-attach <server>` command and do not specify the `net-id` option, the error `Failed to attach interface` is displayed even though the instance is attached to all networks in the project. The OpenStack Compute Service (Nova) also attempts to attach the External Network, which may cause the instance to plug in to the wrong External Network, or may prevent the instance from booting because of a permission issue. 1. From a Windows or Linux system where the OpenStack CLI package for CloudSystem is installed, run the `nova interface-attach <server>` command with at least one of the following options: `net-id`, `port-id`, or `fixed-ip`.
You use the `nova ssh`command to connect to an instance and the connection is made to the Provider Network instead of the floating IP address of the instance	**You are not entering the correct IP address for the instance** 1. Determine the IP address of the instance by viewing the instance details in the CloudSystem Portal, or by running the `nova list` command from a Windows or Linux system where the OpenStack CLI package for CloudSystem is installed. 2. Manually `ssh` to the IP address.

Floating IPs are not working

Symptom	Possible cause and recommendation
You cannot access a virtual machine instance over the External Network using the floating IP address associated with the instance	**The instance does not have the proper security rules assigned** 1. Log on to the CloudSystem Portal. 2. From the **Project** menu in the "Manage Compute" section, select **Instances**. 3. On the **Instances** screen, select the instance. 4. Select **More→Edit Security Groups**. 5. On the **Security Groups** tab of the **Edit Instance** screen, do one of the following • Choose a security rule that allows you to communicate with the instance. • Create a new security rule with PuTTY, SSH, or ping access privileges to match your configuration. See Create a security group (page 118). 6. Retry accessing the instance.
	The instance is connected directly to the External Network 1. Log on to the CloudSystem Portal. 2. From the **Project** menu in the "Manage Compute" section, select **Instances**. 3. On the **Instances** screen, click the link for the instance. 4. On the **Instance Overview** screen, verify that the instance is connected directly to the External Network. 5. Delete the instance. See Delete instance (page 109). 6. Relaunch the instance using a provider or private network. See Launching an instance using CloudSystem Portal (page 119). 7. Associate the private or provider network to the External Network using a logical router. See Creating an External Network router (page 79). 8. Retry accessing the instance.
	The security settings for the Cloud Data Trunk and the External Network port groups on the ESX management hypervisor are not properly configured 1. Log in to vCenter Server. 2. Select the management hypervisor.

Symptom	Possible cause and recommendation
	3. Check the security settings for the Cloud Data Trunk and, if necessary, change them to the following: • `Promiscuous mode: ACCEPT` • `MAS address changes: ACCEPT` • `Forged Transmits: ACCEPT` 4. Retry accessing the instance.
	Changing the initial gateway IP address for the External Network requires recreating a new subnet In the CloudSystem Portal, you can specify a Gateway IP address for the External Network subnet. If you do not specify a value for Gateway IP, it is set to the first IP address in the subnet address pool. However, if you attempt to modify the Gateway IP at a later time, the External Network gateway setting is not changed and, therefore, floating IP access to instances may not succeed if the gateway is involved in the communication path. 1. Log on to the CloudSystem Portal. 2. Delete the External Network subnet. a. From the **Admin** menu in the "System Panel" section, select **Networks**. b. On the **Networks** screen, click the External Network link. c. On the **Network Overview** screen, on the right side of the "Subnets" section, click **+ Delete Subnets**. d. On the **Confirm Delete Subnets** screen, click **Delete Subnets**. e. Verify that the External Network subnet is no longer listed on the **Networks** screen. 3. Create a new External Network subnet, specifying new IP addresses for allocation pools. See Creating the External Network subnet (page 77).
DHCP is enabled, and is not allowing the use of floating IPs on the External Network subnet	**The DHCP option is enabled by default on the External Network subnet** 1. Log on to the CloudSystem Portal. 2. Verify that DHCP is enabled, and that the gateway IP address is not the first address in the allocation pool for the subnet. a. From the **Admin** menu in the "System Panel" section, select **Networks**. b. On the **Networks** screen, click the External Network link. c. On the **Network Overview** screen, on the right side of the "Subnets" section, click **Edit Subnet**. d. On the **Update Subnet** screen, select the **Subnet Detail** tab. e. Examine the **Enable DHCP** setting and the **Allocation Pools** list. 3. Click the **Enable DHCP** check box to clear the option, and then click **Update**. 4. Verify that the gateway IP address is listed as the first address in the **Allocation Pools** list.
You cannot access an instance using a floating IP address when the instance is assigned to a network other than NIC1	Associate a floating IP address to the first NIC on the instance. Do not associate more than one floating IP to an instance.

Changing the External Network address allocation pools fails

Symptom	Possible cause and recommendation
Entering new IP address ranges for the External Network subnet allocation pool fails	**After initial configuration, you must delete and recreate the External Network subnet to associate new allocation pool addresses** 1. Log on to the CloudSystem Portal. 2. Delete the External Network subnet. a. From the **Admin** menu in the "System Panel" section, select **Networks**. b. On the **Networks** screen, click the External Network link.

Symptom	Possible cause and recommendation
	c. On the **Network Overview** screen, on the right side of the "Subnets" section, click **+ Delete Subnets**. d. On the **Confirm Delete Subnets** screen, click **Delete Subnets**. e. Verify that the External Network subnet is no longer listed on the **Networks** screen. 3. Create a new External Network subnet, specifying new IP addresses for allocation pools. See Creating the External Network subnet (page 77).

Networks not recreated after management cluster or hypervisor reboot

Symptom	Possible cause and recommendation
You reboot the management cluster or hypervisor, or edit Cloud Networking settings after the initial setup, and you do not see networks listed on the console or the portal, or the networks are listed with an error status	**After you reboot the management cluster or hypervisor, or edit Cloud Networking settings, CloudSystem may take up to 60 minutes to recreate networks** 1. After rebooting the management cluster or hypervisor, or editing Cloud Networking settings, wait 60 minutes. 2. Verify that the networks are listed on the console or portal, and that there operational status is "active."

Troubleshooting integrated tools

VMware vCenter Server must be configured with English as the default language

Symptom	Possible cause and recommendation
When you run csstart in a browser, you see the error `Pre Installation failed` on the installation screen, and `fault.NicSettingMismatch.summary` in the vCenter Server task information	**Data returned by the vCenter Server does not match what is expected by CloudSystem** The vCenter Server that you specify in csstart or the "Register VMware vCenter Server" dialog on the CloudSystem Console **Integrated Tools** screen must have English as its default language. • Change the language on your vCenter Server to English, or • Manage the CloudSystem management hypervisors using an instance of vCenter Server with English as its default language. This may require that you start a new vCenter Server whose language is English.

VMware vCenter Server registration does not succeed

Symptom	Possible cause and recommendation
When registering VMware vCenter Server on theIntegrated Tools screen, you see `Unable to validate connection to VMware vCenter Server`	To troubleshoot configuration errors, click the **Edit** link to the right of the **VMware vCenter Server** panel on the **Integrated Tools** screen. **VMware vCenter Server address is incorrect** 1. Make sure the FQDN or IP address is correct for the VMware vCenter Server you are trying to register. **VMware vCenter Server port is incorrect** 1. Check the VMware vCenter Server properties and verify that the port number you are using is correct. **VMware vShield Manager details are incorrect** 1. Check the address of the vShield Manager and verify that you are entering the correct address for the security group. 2. Make sure you are entering an authorized user name and password for vShield Manager.
When registering VMware vCenter Server 5.0 Update 3 on the Integrated Tools screen, you see `No Element found`	**Defect in vCenter Server 5.0 Update 3** • Follow the steps in VMware Knowledge Base 2010507: VMware Knowledge Base • Retry the vCenter Server registration again.

You cannot log in to HP Operations Orchestration

Symptom	Possible cause and recommendation
Cannot log in to OO Central using the CloudSystem Foundation	**OO administrator password and CloudSystem Foundation administrator password are not synchronized** The OO administrator password may have changed since CloudSystem Foundation was installed. When CloudSystem Foundation is installed and configured, the OO administrator

Symptom	Possible cause and recommendation
administrator password	password is set to match the Foundation administrator password. If the OO administrator password is changed after installation, then the OO administrator and Foundation administrator passwords are not synchronized. 1. Log in to OO using the most recent OO administrator password. (You may need to obtain the password from the person who changed the OO administrator account.) 2. If you cannot perform step 1, contact HP support for help with resetting the OO administrator password. See How to contact HP (page 41).

HP Operations Orchestration Studio help link displays a blank screen

Symptom	Possible cause and recommendation
Using Google Chrome with OO Studio, you click the help icon and see an empty screen	**Operations Orchestration Studio earlier than 10.02 does not display help in Google Chrome** • Update OO Studio to 10.02. • If you need access to the help topics before you can update OO Studio, use a supported version of Internet Explorer or Firefox. See the *HP CloudSystem 8.0 Installation and Configuration Guide* for information about updating OO Studio and for a list of supported browsers.

Troubleshooting images

TIP: For additional troubleshooting information, enable console access on your Foundation base appliance using the CLI and then find the following logs. To enable access, see Enable console access and set the password (page 199).

- `/var/log/glance/api.log`
- `/var/log/glance/registry.log`

Add image action is unsuccessful

Apply the recommendations that pertain to your situation.

Symptom	Possible cause and recommendation
Windows image is not recognized in vCenter Server	**Custom attributes are not set on the image** Set custom attributes on Windows images (`.vmdk`) from the OpenStack Glance CLI using one of the following methods.

Symptom	Possible cause and recommendation

	• After you upload a Windows image using the **Add Image** screen in the CloudSystem Console, use the Glance CLI to set the attributes on the file.
	On a Windows or Linux system where the OpenStack CLI package for CloudSystem is installed, enter the following command, where *Windows-image.vmdk* is the name of your Windows image to update:
	`glance --insecure image-update --name <Windows-image.vmdk> --property vmware_ostype=windows8Server64Guest --property vmware_adaptertype=lsiLogicsas`
	• When you use the OpenStack Glance CLI to upload the image, you can set the attributes and upload the image at the same time.
	On a Windows or Linux system where you installed the OpenStack CLI package for CloudSystem and which contains the image to upload, enter the following command, where *Windows-image.vmdk* is the name of the Windows image, and *new-Windows-image.vmdk* is the name of the modified image that is uploaded to CloudSystem:
	`glance --insecure image-create --name <Windows-image.vmdk> --disk-format=vmdk --container-format=bare --file <new-Windows-image>.vmdk --property vmware_ostype=windows8Server64Guest --property vmware_adaptertype=lsiLogicsas`
	See also Setting custom attributes on Microsoft Windows images (page 85).
	For more information, see OpenStack glance commands at OpenStack Cloud Software.

When uploading an image, `Error adding image` is displayed	**Disk space allocated for image is full** 1. Increase the storage volume by expanding the logical volume for the storage file system, or clean up used disk space. **Image to be uploaded has the same identifier as another image** 1. If there are duplicate identifiers, delete one image or create a new image with a different (unique) identifier. Now retry the **Add Image** action. If the error persists, download and check log files. From the **Settings** screen, select **Actions→Download audit logs**.
The size of the uploaded image is smaller than expected on the Images screen	**The image upload was only partially completed due to browser upload size limits** This might be the source of the problem if: • The image file is more than 4 GB and your browser is Microsoft Internet Explorer or Mozilla Firefox • The image file is more than 20 GB and your browser is Google Chrome In this situation, 1. Manually delete the image using the **Delete** action, which deletes the image entry from the database. 2. Place the image on a file server. 3. Retry the **Add Image** action and **Enter file URL**. This option allows you to add a pointer to the image on the file server, which will be used to locate the image during provisioning.
After adding an image, you created an instance from the image. The instance has an Active state but a 0 size	**You specifed the URL of a folder that does not contain an image file** When you upload an image in the CloudSystem Console, the OpenStack Image Service (Glance) allows you to specify the URL of a folder that does not contain an image file. A warning or error message is not displayed. • Delete the image that is a folder instead of a file, and add the correct image using the **Add Image** screen, or • Add the correct image by entering the following command on Windows or Linux system where the OpenStack CLI package for CloudSystem is installed. `glance image-create`

Symptom	Possible cause and recommendation
The status of a recently uploaded image is "Killed"	**You navigated away from the Add Image screen in your browser while the image was uploading** 1. Manually delete the image using the **Delete** action, which deletes the image entry from the database. 2. Retry the **Add Image** action. **The disk became full while the image was uploading** 1. Manually delete the image using the **Delete** action, which deletes the image entry from the database. 2. Verify whether or not the disk space for image storage is full. Increase the storage volume by expanding the logical volume for the storage file system, or clean up used disk space. 3. Retry the **Add Image** action.
You see `Error contacting image service` when uploading an image	**Access permission for storage media might be incorrect** 1. Verify permissions for the storage media, and correct as needed. 2. Retry the **Add Image** action. If the error persists, download and check log files. From the **Settings** screen, select **Actions→Download audit logs**.
The image remains in the "Uploading" state indefinitely	**The Glance image service stopped or restarted while the image was uploading** 1. Check the size of the image on the file server and the time it started uploading on the **Activity** screen. If the image size is less than 10 GB and it has been uploading from a file server for more than 30 minutes, it might be in an indefinite upload state. (An image uploaded from your local system through your browser might take much longer to complete.) 2. If it appears that the image upload will not complete, select the image and delete it using the **Delete** action. 3. Retry the **Add Image** action.

Create image action is unsuccessful

Symptom	Possible cause and recommendation
When you select Create Image from the CloudSystem Console Instances screen, the operation is unsuccessful	**Creating an image from a running ESX instance does not succeed** 1. Do not use the Create Image action from the CloudSystem Console **Instances** screen. 2. Use the other methods to upload an image, including adding an image from the **Images** screen and using the OpenStack Glance CLI.
You see an indication that the compute node capacity has been exceeded	**Oversubscription rates might be incorrect for the load on the virtual and physical servers** 1. Verify the physical to virtual oversubscription rates. See Calculating the number of instances that can be provisioned to a compute node (page 105).

Edit image action is unsuccessful

Apply the recommendations that pertain to your situation.

Symptom	Possible cause and recommendation
You see `Error getting image` when editing an image	**The image is set to "Read Only"** 1. Ensure that the image **Protected** setting shows "Read-Write." 2. Retry the **Edit Image** action. **Other image settings or the image itself are incorrect** 1. Ensure that the image metadata is correct and that the image is valid. If the image is not valid, you will need to recreate it. 2. Retry the **Edit Image** action. If the error persists, download and check log files. From the **Settings** screen, select **Actions→Download audit logs**.

Image server storage configuration is unsuccessful

Apply the recommendations that pertain to your situation.

Symptom	Possible cause and recommendation
You see `Error occurred during image server storage configuration`	**Dedicated glance storage volume is not available for mounting at startup** 1. Ensure that there is a device named `/dev/sdb` and that it is accessible to the appliance VM that was configured during initial installation. 2. Download and check log files for additional information. From the **Settings** screen, select **Actions→Download audit logs**. If the error persists, contact your storage administrator.

Base folder of the ESX cluster shared datastore may contain files related to unused images

Symptom	Possible cause and recommendation
You see unused image files in the ESX cluster shared datastore	**Files related to unused images are not cleared** • To free space, manually delete the unused image files from the base folder of the ESX cluster.

Using the OpenStack Glance API to upload an image may not succeed when CloudSystem Foundation is first installed

Symptom	Possible cause and recommendation
When you upload an image using the OpenStackGlance API, you see `Failed to configure store correctly: Store cinder could not be configured correctly. Reason: Cinder storage requires a context. Disabling add method`	**CloudSystem Foundation is not fully up and running** • From the **Actions** menu on the CloudSystem Console **Settings** screen, select "Reboot Foundation appliances." • Retry adding the image.

Troubleshooting storage

TIP: For additional troubleshooting information, enable console access on your Foundation base appliance using the CLI and then find the following log. To enable access, see “Enable console access and set the password” (page 199).

- /var/log/cinder/volume.log

For more information, see the *HP 3PAR StoreServ Storage Troubleshooting Guide* available from the *HP Support Center* at http://www.hp.com/go/support.

Increase 3PAR storage systems connection limit

Symptom	Possible cause and recommendation

OpenStack Block Storage servers cannot connect to the 3PAR storage system	**The default connection limit has been reached**
	The web service supports up to 15 connections, so there can be up to 15 OpenStack Block Storage servers enabled to access the 3PAR storage system. However, the default number of allowed connections is lower. .
	• Increase the connection limit to15 by opening an ssh connection to the 3PAR storage system and entering:
	`% setwsapi -sru high`
	`% showwsapi -sru`
	The following will be displayed:
	`WSAPI server SRU is set to: high (15)`

Cinder block storage volume does not attach to virtual machine instance

Symptom	Possible cause and recommendation
3PAR iSCSI volume does not attach to virtual machine instance, and the volume state reverts to Available	**Incorrect compute node connectivity configuration** 1. Confirm the connectivity configuration from the targeted compute node to the 3PAR storage system. See HP 3PAR StoreServ Storage documents (page 43) for additional information. 2. Retry the connection. **Insufficient storage on the 3PAR system** 1. Check the available storage on the 3PAR storage system to which you want to attach, and allocate additional capacity if needed. 2. Retry the connection. **Invalid FQDN name** 1. The compute node server name in vCenter Server must be a unique FQDN. Enter a valid fully qualified domain name for the 3PAR storage system to which you want to attach. 2. Retry the connection. **The volume name you created is already being used** 1. Create a unique volume name that is not duplicated. Each volume name is used with a different target. 2. Retry the connection. **The World Wide Name (WWN) for the server host bus adapters (HBA) in 3PAR ends in zero (0)** 1. Change the WWN for the server HBAs in 3PAR. The name cannot end with a zero (0). See HP 3PAR StoreServ Storage documents (page 43) for additional information. 2. Retry the connection. **The REST API is not enabled on the 3PAR system** 1. Enable the REST API on the 3PAR storage system you want to attach. See HP 3PAR StoreServ Storage documents (page 43) for additional information. 2. Retry the connection. 3. If this does not correct the problem, forward the following files and logs to HP: • csbase appliance • /var/log/cinder/volume.log • vProxy server (ESX compute attach issues) • /var/log/nova/compute.log
When a cinder block storage volume does not attach to a VM instance, you see the following error in the `/var/log/cinder/volume.log` **file:** `Error: Everything must be in the same domain to perform this operation. Objects belonging to <domain_name> domain and to <domain_name> were specified.`	**Multiple virtual domains are defined on the 3PAR storage system** 1. Edit the storage virtual domain to be in the same location as the compute server storage location. See HP 3PAR StoreServ Storage documents (page 43) for additional information. 2. Verify that the domains are displayed in the **Domains** drop-down selector on the **Add block storage driver** screen. See Add Block Storage Drivers (page 89).
Unable to determine reason for the volume not attaching to a VM instance	**Debugging required** 1. If after trying all of the above actions the volume still will not attach, enable debugging in the log files on the compute nodes

Symptom	Possible cause and recommendation
	(`/var/log/nova/compute.log`) and the appliance (`/var/log/cinder/volume.log`). 2. Also check the `/var/log/ciDebugLogxxx.log` and `/var/cinder/scheduler.log` files for possible clues. 3. Search foran error in the log files to determine the issue. 4. If you still are unable to determine the problem, forward the log files to HP.

Cinder block storage volume does not establish an SSH connection with the 3PAR storage system

Symptom	Possible cause and recommendation
You see the error: `3PAR_SSH_CONNECTION_FAILURE`	**The base appliance is unable to establish SSH connection with the 3PAR storage system** 1. Retry the request. 2. If the error persists, verify that SSH connections to the 3PAR storage system can be established from the base appliance, and then try the request again. **The base appliance is unable to establish an HTTPS connection with the 3PAR storage system** 1. Retry the request. 2. If the error persists, re-import the 3PAR SSL certificate into the base appliance, and then retry the request.
You see the error: `3PAR_SSH_CONNECTION_KEY_MISMATCH_FAILURE`	**The host key has changed** **NOTE:** The host key can change when upgrading firmware, or if CloudSystem Console security is compromised. 1. Manually verify that the correct 3PAR SSH host key is installed on the base appliance.

Specifying a device already in use causes an error when attaching a volume

Symptom	Possible cause and recommendation
• **If you specify a device already in use or an ESX reserved device (`/dev/vdh`, `/dev/sdh`, `/dev/vdp`, and `/dev/sdp`), the operation does not succeed and the volume is not attached to the instance** • **If you specify a device not in use, the specified device is not necessarily attached**	**The guest operating system allocates the next available device name to attach to the volume** • Using the CloudSystem Portal, you must specify a device. For example, enter `/dev/sdc` for ESX and `/dev/vdc` for KVM. **NOTE:** Do not specify a device that is currently in use. However, the device you specify is not necessarily the device that is attached. When the volume is attached, log in to the deployed instance operating system and view the device information for the instance. The volume details in the CloudSystem Portal reflect the device initially used while attaching the volume, but do not necessarily reflect the final device as seen by the operating system. • Using the the OpenStack CLI, use the “auto” option to allow Nova to automatically select the device name. For example: `nova volume-attach <instance-ID> volume auto` • Using the OpenStack API, use the “device null” option.

Volume not associated with a volume type cannot be modified or deleted when the storage driver is removed

Symptom	Possible cause and recommendation
The volume state of "deleting" does not change on the **Volumes** screens in the CloudSystem Portal and the CloudSystem Console.	**When the volume was originally created no volume type was explicitly associated with the block storage driver.** **NOTE:** When a volume is created without an associated volume type and driver, OpenStack Cinder automatically assigns a valid block storage driver to the volume. In this situation, the volume cannot be deleted or modified if the assigned driver is deleted. Attempting to delete or modify the volume puts the volume in a hung state. 1. To remedy the problem from the CloudSystem Portal, add the same driver type to the volume using the same IP address. See Add Block Storage Drivers (page 89). 2. When deleting block storage drivers, be sure to first delete the volumes until the **Block Storage Drivers** overview screen in the CloudSystem Console displays 0 in the **Block storage volumes** column of the **Host CPG Summary**.

Volume is in Error state when it is created without a block storage driver

Symptom	Possible cause and recommendation
You cannot attach a volume in the `Error` state to a virtual machine instance	**You created a volume in the CloudSystem Portal before you created a Fibre Channel or iSCSI block storage driver in the CloudSystem Console** • Delete volumes in an Error state using the CloudSystem Portal or CloudSystem Console. To prevent volumes from becoming unusable, perform the following actions in order: 1. Add a block storage driver in the CloudSystem Console. 2. Add a volume type in the CloudSystem Console, and associate the volume type with a block storage driver. 3. Create a volume in the CloudSystem Portal or using the OpenStack Cinder CLI.

Unable to associate block storage driver with 3PAR storage system

Symptom	Possible cause and recommendation
When adding or editing a block storage driver, the driver is unable to be associated with the 3PAR storage system	**Missing or incorrect user ID and password combination** 1. Enter a valid user ID and password for the 3PAR storage system to which you want to associate the driver. 2. If this corrects the problem an additional section is displayed on the **Add Block Storage Driver** screen or the block storage driver **Edit** screen. **Missing or invalid FQDN or IP address** 1. Enter a valid fully qualified domain name or IP address for the storage system to which you want to associate the driver. 2. If this corrects the problem an additional section is displayed on the **Add Block Storage Driver** screen or the block storage driver **Edit** screen.

Unable to delete block storage driver

Symptom	Possible cause and recommendation
When trying to delete a block storage driver, you see the message: `A block storage driver that has dependent volume types cannot be deleted. You must delete the following volume types before deleting the block storage driver.`	**The driver that you are trying to delete is associated with one or more volume types** 1. Delete the associated volume type(s), and retry the delete driver action. See Delete Volume Types (page 93). 2. With the filters set to **All statuses**, verify that the volume type no longer appears in the list on the **Block Storage Drivers** overview screen.

Unable to delete a volume type

Symptom	Possible cause and recommendation
When trying to delete a volume type you see the message: `A volume type that has dependent volumes cannot be deleted. You must delete the following volumes before deleting the volume type.`	**The volume type that you are trying to delete is associated with one or more volumes** 1. Delete the associated volume(s), and retry the delete volume type action. See Delete Volumes (page 95). 2. With the filters set to **All statuses** and **All driver types**, verify that the volume type no longer appears in the list on the **Volume types** overview screen.

Unable to edit a volume type

Symptom	Possible cause and recommendation
When trying to edit a volume type, you see the message: `Volume types created outside CloudSystem Console, for example using the Cloud Storage admin CLI, cannot be edited by CloudSystem Console.`	**The volume type that you are trying to edit was created outside of the CloudSystem Console** 1. Use the CloudSystem Console to delete the volume type. See Delete Volume Types (page 93). 2. Use the CloudSystem Console to add the volume type. See Add Volume Types (page 92). 3. Use the CloudSystem Console or Cloud Service Management Console to edit the volume type. See Edit Volume Types (page 93).

Volume created with a failed block storage driver cannot be deleted

Symptom	Possible cause and recommendation

You cannot delete a volume created with a valid block storage driver using the CloudSystem Console or CloudSystem Portal	**The associated block storage driver failed or is unconfigured by editing cinder.conf**
	• Reset the state using the following OpenStack Cinder command from a Windows or Linux system where the OpenStack CLI package for CloudSystem is installed:
	`cinder reset-state <volume name or ID>`
	If delete is the desired state, follow the preceding command by entering:
	`cinder force-delete <volume name or ID>`

Volume status is mismatched between CloudSystem Console and CloudSystem Portal

Symptom	Possible cause and recommendation
The current volume status that is displayed in the CloudSystem Portal is different than the status displayed in the CloudSystem Console	**The volume status displayed in the CloudSystem Console refreshes only once per hour with data from the CloudSystem Portal** 1. No action is required. Always refer to the status displayed in the CloudSystem Portal for the most current volume status. The hourly refresh will update the status in the CloudSystem Console.

Renaming or changing the comment section in volumes with an “osv-” prefix in the 3PAR storage system causes the volumes to become inoperable

Symptom	Possible cause and recommendation
A volume is inoperable and is deleted when you run the CloudSystem recovery procedure	**You renamed a volumes with an “osv-” prefix or removed its comment section in the 3PAR storage system** When you create a block storage volume in the CloudSystem Portal or using the OpenStack Cinder CLI, the names of the volume in the 3PAR storage system is prefixed with `osv-`. • Delete the volume and recreate it in the CloudSystem Portal or using the OpenStack Cinder CLI.

Block storage volumes may indefinitely remain in undesired state

Symptom	Possible cause and recommendation

Volume is stuck in an undesired stated (detaching, deleting, attaching, and so on) for a period of time	**Various possible issues in OpenStack Block Storage (Cinder) or 3PAR storage system**
	• Reset the state using the following OpenStack Cinder command from a Windows or Linux system where the OpenStack CLI package for CloudSystem is installed:
	`cinder reset-state <volume name or ID>`
	If delete is the desired state, follow the preceding command by entering:
	`cinder force-delete <volume name or ID>`

Last iSCSI initiator configured for an ESX host is used for attaching a volume

Symptom	Possible cause and recommendation
You configured more than one hardware or software iSCSI initiator on an ESX host, but only the last initiator that was configured is used when the volume is attached	**Interaction between CloudSystem and ESX** • Configure only one iSCSI initiator for an ESX host.

Attaching an iSCSI volume to an ESX instance slows if degraded LUNs exist in vCenter Server

Symptom	Possible cause and recommendation
Attaching an iSCSI volume to an ESX instance takes several minutes	**LUNs in a degraded state cause extra rescans in the vCenter Server** • Clean up the vCenter Server by removing LUNs in a degraded state, then retry the attach operation.

Volume state is not immediately updated when deleting a volume does not succeed

Symptom	Possible cause and recommendation
When deleting a volume in the CloudSystem Console, the volume state is not changed from "Deleting" to "Error_Deleting" for approximately 2 to 5 minutes	**Communication between the storage system and the CloudSystem Console** • View the volume state in the CloudSystem Portal, which is updated immediately, or • Wait a few minutes, then refresh the **Volumes** screen in the CloudSystem Console to display the latest volume state.

Block storage drivers Host CPG summary is not automatically updated

Symptom	Possible cause and recommendation
• **You do not see updated information in the Host CPG Summary table on the Block Storage Drivers Overview screen when a volume type or volume is created or a common provisioning group (CPG) is added or removed** • **If you select a different block storage driver, the Host CPG Summary table does not change to reflect CPG information for the new driver**	**Data is not dynamically refreshed** If you view the General, Storage System Access, Details, or Utilization screens, the Host CPG Summary table is not dynamically refreshed when you return to the Overview screen. • Refresh the Block Storage Drivers Overview screen.

Troubleshooting compute nodes

Compute nodes do not appear on overview screen

Symptom	Possible cause and recommendation

No KVM compute nodes are visible on the Compute Nodes overview screen	**No KVM compute nodes are configured for use**
	1. Make sure that all prerequisites have been met for each target compute node.
	The KVM compute node network configuration is incorrect
	1. Run `ifconfig` to check the network configuration on the compute node. The DHCP server on the CloudSystem Console appliance must recognize the compute node.
	2. If the compute node is connected to the appliance (eth1 has a valid DHCP IP address), edit the file `/etc/sysconfig/networks` on the compute node with the following entries:
	`NETWORKING=yes`
	`HOSTNAME=<change-name>`
	`DHCP_HOSTNAME=<NON-FQDN>`
	Local yum repositories are causing issues
	1. Remove any locally defined yum repositories that may be interfering with activation.
	2. When reactivating a compute node, make sure any leftover active yum repositories are removed.
	The CloudSystem Console is displaying cached data
	1. Refresh the Compute Nodes screen.
	TIP: Check the following logs for additional information:
	• Foundation base appliance: `/var/log/isc/activity <yourhostname>.log`
	• KVM compute node: `/var/log/secure`

Import cluster action does not complete

TIP: For additional troubleshooting information, enable console access on your Foundation base appliance using the CLI and then find the following logs. To enable access, see Enable console access and set the password (page 199).

- `/etc/pavmms/deployer.conf`
- `ci/logs/ciDebug.01.log`
- `ci/logs/jetty-PulsarAVMManager/server.log`

Symptom	Possible cause and recommendation
Import cluster action cannot complete in CloudSystem Console	**DHCP server is not defined on the Data Center Management Network** 1. Make sure the Data Center Management Network configured on the management hypervisor is set to use **DHCP** for IP address assignment. 2. Log in to the CloudSystem Console and make sure the proxy appliance registered in Integrated Tools is set to receive IP addresses from DHCP. • From CloudSystem Console main menu select **Integrated Tools**. • Find the **VMware vCenter Server** panel on the screen. • Make sure the line **IP addresses for proxy appliances** is set to **DHCP**. • If DHCP is not set, click the link to open the **Plan vCenter Access** screen. • Select **DHCP**. 3. Retry the **Import cluster** action.

Activate compute node action is unsuccessful

TIP: For additional troubleshooting information, enable console access on your Foundation base appliance using the CLI and then find the following logs. To enable access, see Enable console access and set the password (page 199).

- `/var/log/isc/activity.<hostname>.log`

Symptom	Possible cause and recommendation
You see an error on the Activity screen when you try to activate a cluster or compute node	**Prerequisites for activation have not been met** 1. Make sure that all prerequisites have been met. **The cluster was created in a vCenter Server folder** 1. Create clusters directly under the Datacenter and not inside a folder. 2. Retry the activate action. **The user name and password for the operating system on the KVM compute node might be incorrect** 1. Make sure that the user name and password are entered correctly in the Activate dialog when activating the KVM compute node. 2. Retry the activate action. **Operating system installation on the KVM compute node may be incorrect** 1. Make sure that the activation base image was installed correctly by RedHat Package Manager (RPM). 2. Retry the activate action.

Symptom	Possible cause and recommendation
	VM host was recently moved into or out of Maintenance mode 1. In the CloudSystem Console, select **Integrated Tools** from the main menu, then open the Edit VMware vCenter Server screen and click Save. 2. Retry the activate action. **The cluster or compute node might be rebooting** 1. Check the status on the **Compute Nodes** screen. 2. Wait for a reboot to complete. The status icon will be green. 3. Retry the activate action.
KVM compute node activation fails or hangs and no error message is displayed	**A dependency on the KVM compute node was not met** 1. Log on to the KVM compute node and obtain a support dump. The detailed activation log is in `/var/log/isc/activation<hostname>.log` 2. Scroll through the log and find the start of the roll back procedure. The error details are displayed just above the start of the roll back procedure. **An activated compute node was selected for activation again and is not responding** 1. Log on to the KVM compute node. 2. Open `/etc/yum.repos.d` and set all repositories to `enabled=0`. 3. Switch to the CloudSystem Console and retry the **activate** action.

KVM compute node activation fails with `Neutron client authentication failed: Connection to neutron failed: timed out. Getting disk size of instance-00000001: [Errno 2] No such file or directory` in the nova log file.	**RHEL 6.4 compute node default kernel value must be increased**
	Configure KVM compute nodes with a be2net NIC driver so that the `rx_frag_size` kernel parameter value is set to 8192. (The default is 2048.) This setting avoids packet loss and network communication drop issues.
	1. Check for the be2net NIC driver by entering the following command on the KVM compute node command line:
	`# ethtool -i eth0`
	If the driver is loaded, you see `driver: be2net`.
	2. If the be2net driver is loaded, check for the current `rx_frag_size` value by entering:
	`# cat /sys/module/be2net/parameters/rx_frag_size`
	3. If the value is less than 8192, set the value to 8192 by adding the following line in the file `/etc/modprobe.d/be2net.conf` on the compute node. If the file does not exist, create it, then add the following line.
	`options be2net rx_frag_size=8192`
	4. Reboot the compute node.

Deactivate compute node action is unsuccessful

Symptom	Possible cause and recommendation
You see an error on the Activity screen when you try to deactivate a compute node	**The managed compute node is not been activated** 1. Ensure that the compute node is activated. An active compute node displays a green icon. **One or more virtual machines are running on the compute node** 1. Make sure there are no virtual machine instances running on the compute node. If an instance is running on the compute node, you must delete the instance before you can deactivate the compute node. To delete an instance, select **Instances** from the main menu, then select **Actions→Delete**. 2. Retry the deactivate action. See Deactivate a compute node (page 106).
The compute node fails when you try to deactivate it	**Deactivation log files might have exhausted the compute node disk volume space** 1. Bring the compute node back up. 2. Make sure that the log files are written to a physical volume other than the boot disk. You should have assigned a log location prior to activating the host. 3. Check the size of the log files in the `/var/log/nova` directory. Delete the files if they are consuming too much space on the disk. 4. When sufficient log file space is available, try again to deactivate the compute node. See Deactivate a compute node (page 106).

Delete compute node action is unsuccessful

Symptom	Possible cause and recommendation
You see an error on the Activity screen when you try to delete a compute node	**The compute node has not been deactivated** 1. Ensure that the compute node is deactivated. A deactivated compute node displays a red icon. See Deactivate a compute node (page 106). 2. Retry the delete action. See Delete a compute node (page 107).

Red Hat netcf bug fix update corrects libvirt issues

Symptom	Possible cause and recommendation
libvirt crashes with a segmentation fault	**Red Hat `netcf` bug fix update is required** On KVM compute nodes running RHEL 6.4 or 6.5, running simultaneous VM operations for long periods of time may cause libvirt to crash with a segmentation fault. • Update the KVM compute node with the `netcf` bug fix update from Red Hat. For detailed information, see http://rhn.redhat.com/errata/RHBA-2014-0263.html.

Troubleshooting virtual machine instances

TIP: For additional troubleshooting information, enable console access on the Foundation base appliance using the CLI and then find the following logs. To enable access, see Enable console access and set the password (page 199).

- `/var/log/nova/scheduler.log`

You can also access the following logs on the Proxy appliance:

- `/var/log/nova/compute.log`
- `/var/log/sdn/isc-neutron-agent.log`

Deployed instance does not boot

Symptom	Possible cause and recommendation
After you add an ESX host to an activated cluster, the status of a newly created ESX instance is "Error"	**Shared storage among all of the hosts in the cluster does not exist** • Ensure that all hosts in the cluster, including the new host, shares data store(s). **Instance cannot access the network** • Ensure that a VMware vSphere Distributed Switch (VDS) is defined for the new host added to the cluster. See the *HP CloudSystem 8.0 Installation and Configuration Guide* at Enterprise Information Library.
You see `Unable to create instance. No available host can provide the specified resources`	**No compute nodes in active state** • Navigate to the Compute Nodes screen and ensure that at least one compute node is in the Active state. See Activate a compute node (page 105). **Insufficient resources available on active compute nodes** 1. Check the error message on the **Activity** screen for the unsuccessful instance. The event describes the type of host (QEMU or VMware) and the resources required by that instance. 2. Ensure that you have sufficient cloud resources on the compute node. On the Compute Nodes screen, verify the number of hosted VMs, CPU, memory, and storage usage and compare those values to the resources that will be allocated to the instance. If sufficient resources are not available: • Add compute resources to the compute node. • Free space on the compute node by deleting existing cloud instances. • Verify the physical to virtual oversubscription rates. See Calculating the number of instances that can be provisioned to a compute node (page 105) **NOTE:** The Compute Nodes screen displays the percent of resources in use and the total amount of resources. However, the actual available resources of a compute node are calculated by subtracting allocated resources (the virtual machine instances already provisioned to a host) from the capacity of the compute node. Note the number of **hosted virtual machine instances** when evaluating whether resources on a particular compute node are available, even if the instances are not consuming all allocated resources or are powered down. If one or more virtual machine instances in a host are powered down, the compute node appears to have a high percentage of free resources, but the available resources are actually already allocated to the powered down instances. Additionally, the **storage allocation percentage** does *not* include • The reserved storage for the image cache, which is 10% of the total storage size available for the compute node • The space occupied by the operating system, if it is residing on the same volume • Pre-existing instances that were not provisioned by CloudSystem

Launch of first instance provisioned from ESX does not complete

Symptom	Possible cause and recommendation
The first attempt to launch an instance provisioned from ESX does not complete	**Virtual machine is created on the hypervisor but provisioning fails due to vSwitch configuration issue** 1. Log in to vCenter Server. 2. Select the compute hypervisor and click the **Configuration** tab. 3. Click **Networking** in the left menu. 4. Make sure the standard or distributed vSwitch has a unique name in vCenter Server. You cannot have two vSwitches in vCenter Server with the same name. **Insufficient resources available on the hypervisor** 1. Log in to vCenter Server. 2. Check the Tasks and Events log for the hypervisor. 3. Add additional resources, if needed. **Datastore does not have enough space** 1. Log in to vCenter Server. 2. Check the available space on the datastore supporting the compute hypervisor. 3. Add additional space, if needed. **Datacenter, hypervisor or vSwitch names have white space** 1. Log in to vCenter Server. 2. Check the names of the datacenter, hypervisor and vSwitch. 3. If the name has white space, update the name to remove the white space.

Booted instances cannot get IP address in ESX environment with vCNS

Symptom	Possible cause and recommendation
You cannot connect to (ping or ssh) booted instance in an ESX environment configured with VMware vCNS	**In the managed VMware vCenter Server, the "vCloud Networking and Security Advanced" license is not applied or the license is expired** 1. From your browser, log in to vShield Manager. 2. In Settings & Reports, Configuration tab, vCenter Server section, check the date and time of "Last successful inventory update" and verify it is current. 3. Verify that the vShield Manager appliance was created and is up and accessible. **vShield Manager appliance is not running** 1. From your browser, log in to vShield Manager. 2. Check that the vShield App appliance is configured properly on each of the hosts. a. On the host on which vShield App is installed, check the "Installed" status of the vShield App service and verify that there are no errors. b. If you see the `DvFilter module is not up on the host` error, restart the vShield Manager. For more information, see the VMware vCloud Networking and Security Documentation at VMware.

Moving a virtual machine with an additional attached volume using vMotion in vCenter Server does not succeed

Symptom	Possible cause and recommendation
You attempt to live move a virtual machine with an additional attached volume and you see `Virtual Disk 'X' is a mapped direct access LUN that is not accessible`	**LUN presentation is not consistent for every host in the cluster** • Follow the instructions in the VMware Knowledge Base 1016210 at VMware.

Delete instance action only partially completes when compute node is unresponsive

Symptom	Possible cause and recommendation
You see `Warning: This instance is on a host that is not responding`	**CloudSystem has lost communication with the server that is hosting the virtual machine instance** Deleting an instance triggers an action on both the CloudSystem Foundation base appliance and the compute node. If the compute node is unresponsive, deleting an instance is only partially completed and requires manual cleanup. 1. Click **Cancel** to return to the previous screen without deleting the instance. 2. Try to restore communication by rebooting the host shown in the "Hosted on" field of the instance. If the host recovers, the instance can be cleanly deleted using the "Delete" action on the **Instances** screen. A *clean* delete removes the instance from both the Foundation appliance database and the host. 3. If the host is in an unrecoverable state (on the **Compute Nodes** screen, the state of the host is "Error"), return to the **Instances** screen. Select the instance, select the "Delete" action, and click **Yes, delete** when the warning message is displayed. **IMPORTANT:** This performs a *partial* delete, which removes the instance from the Foundation appliance database but does not remove the instance from the compute node. After a partial delete, you must clean up the environment as follows: • Manually delete all instances on the compute node. • From the **Compute Nodes** screen, select the compute node and deactivate it. See Deactivate a compute node (page 106). • Check the size of the log files in `/var/log/nova` directory and delete them if they are consuming disk space needed for the next activation or for other use. • Remove the server blade from the cloud. 4. Reinstall the operating system and reactivate the host, if desired. See Activate a compute node (page 105)

Deleting an instance and removing it from the database may cause the instance to remain in the Building state

Symptom	Possible cause and recommendation
When you delete an instance and manually remove it from the database, it remains in the "Building" state	**The OpenStack Compute Service (Nova) driver continues to try to create the deleted instance** • Occasionally, a task may become orphaned. Orphaned tasks cannot be deleted by any user. These tasks are automatically removed from the appliance within 180 days of last modification. • As a best practice, do not attempt to perform operations on instances on the vCenter Server or KVM host. Use the CloudSystem Console and CloudSystem Portal to manage instances.

Create instance runs indefinitely when the Foundation base appliance is rebooted

Symptom	Possible cause and recommendation
You see the unchanging status of a created instance as "Build" in the CloudSystem Portal and "Running" in the CloudSystem Console	**The CloudSystem Foundation base appliance was rebooted while the instance was being created** • Delete the instance in the CloudSystem Portal. • Create the instance in the CloudSystem Portal again.

Soft rebooting a "Shutoff" instance or instance in the CloudSystem Portal causes instance error

Symptom	Possible cause and recommendation
• **In the CloudSystem Portal, when you select an instance in the shutoff state and you click "Soft Reboot Instances," the instance goes into an error state and cannot be subsequently powered up** • **If you attempt to soft reboot the instance in an error state, you see the misleading error `You do not have permission` and the instance is not rebooted**	**OpenStack Compute (Nova) does not prevent rebooting a shutoff instance** 1. Use the OpenStack Nova CLI to reset the status of the instance. Enter the following command on a Windows or Linux system where the OpenStack CLI package for CloudSystem is installed: `nova stop <instance id>` 2. Reboot the instance again.

Instance running on ESX compute node cannot be paused

Symptom	Possible cause and recommendation
When you select "Pause Instance" in the CloudSystem Portal, you see "Success: Paused instance" but the instance is still active	**The pause action is not supported in ESX** • Note that an ESX instance cannot be paused.

Resizing an instance does not succeed when a volume is attached to the instance

Symptom	Possible cause and recommendation
When you select "Resize Instance" In the CloudSystem Portal, you see an error if a volume is attached to the instance	**Implementation error** 1. Detach the volume from the instance. 2. Re-size the number of CPUs or amount of memory of the instance. 3. Reattach the volume.

Launching an instance results in error state

Symptom	Possible cause and recommendation
When you attempt to launch an instance in the CloudSystem Portal, the launch does not succeed and the instance is shown in an Error state	**Error in OpenStack Compute (Nova)** 1. Check the file `/var/log/nova/compute.log` for the error `NoPermission occurred in the call to RetrievePropertiesEx`. 2. Retry the Launch Instance action.

29 Troubleshoot CLI errors

Troubleshoot csadmin

See Working with the csadmin CLI (page 192) for detailed information about csadmin commands.

- Certificate verification errors (page 183)
- Host or proxy connection errors (page 184)
- csadmin –version does not display the correct version number (page 184)
- Some options returned by csadmin –help are not supported (page 184)

Certificate verification errors

Symptom	Possible cause and recommendation

Your command terminates with one of the following messages:
• `Certificate verification failed.`
• `Certificate file does not exist in the specified folder.`
• `Certificate file is invalid.`
	You do not have the root CA certificate for your CloudSystem base appliance saved in the correct location
	NOTE: The following procedure describes saving the certificate using Google Chrome. Your steps may vary if you are using a different browser.
	1. On a Windows or Linux system where `csadmin` is installed, open your browser.
	2. Enter the URL of the CloudSystem Console. You do not need to log in to the console.
	3. Right-click on the padlock icon in the beginning of the URL field.
	A dialog box stating that the identify of the URL is not verified appears with the **Connections** tab selected.
	4. Click the **Certificate information** link.
	The **Certificate** dialog opens.
	5. Select the **Certification Path** tab.
	6. Select the root of the certificate path.
	NOTE: You must select the root of the certificate path rather than the host name of your base appliance. The root path is listed above the host name of your base appliance.
	7. Click **View Certificate**.
	Another **Certificate** dialog opens.
	8. Select the **Details** tab.
	9. Click **Copy to File...**.
	The **Certificate Export Wizard** dialog opens.
	10. Click **Next**.
	11. Select **Base-64 encoded X.509 (.CER)** as the file export format.
	12. Click **Next**.
	13. Enter, or browse to, the file name where you want to save the certificate.
	14. Click **Next**, and then click **Finish**.
	15. Click **OK** three times to close the certificate dialogs.
	16. Open a command window and navigate to the directory where you saved the certificate in step 13.
	17. Enter a `csadmin` command with the `--os-cacert <cert>` argument, where `<cert>` is the name of your certificate file. For example:
	`csadmin appliance list --os-cacert mycert.cer`
	18. Verify that the error condition is resolved by entering a new command.
	NOTE: In environments where security is not a concern, you can suppress these certificate validation errors by appending the `--insecure` option on the `csadmin` command line. For example:
	`csadmin appliance list --os-cacert mycert.cer -insecure`
	See also Optional common arguments (page 193).

Host or proxy connection errors

Symptom	Possible cause and recommendation

Your command terminates with one of the following messages:
• `ERROR: HTTPSConnectionPool(host=' ', port-443): Max retries exceeded with url: https:///rest/login-sessions (Caused by : [Errno 113] No route to host)`
• `ERROR: Response Code: 503 Untrusted SSL Server Certificate`
• `CRITICAL: Exception raised during certificate request... ERROR: Cannot connect to proxy. Socket error: Tunnel connection failed: 503 Service Unavailable`
	Incorrect variable for the CloudSystem host
	1. Determine the IP address of the CloudSystem base appliance.
	2. Retry the command, making sure you append the `--os-auth-url` argument by entering the correct IP address for the `<auth-url>` variable. For example:
	`--os-auth-url http://10.x.x.x/rest/identity/v2.0`
	Incorrect proxy environment variable
	1. Determine if your proxy environment (`env`) variable settings are incorrect. The variable must be:
	• Prefixed with `https://` rather than `http://`.
	• Correctly formatted. For example:
	`https_proxy=https://web-proxy.anyserver1.com:8080`
	2. Reset your proxy environment variable using correct formatting.
	3. Retry the command.

csadmin --version does not display the correct version number

Symptom	Possible cause and recommendation
Entering `csadmin --version` returns 1.0	**csadmin was not updated** • View the correct version number on the **Settings** screen of the CloudSystem Console, for example, 8.0.0.20.

Some options returned by csadmin –help are not supported

Symptom	Possible cause and recommendation
• **Entering `csadmin –help` returns options that are unsupported** • **Specifying these options results in an error**	**csadmin `--os-cert`, `--os-key` and `--os-hp-cs-api-version` are not supported** • Retry the csadmin command without specifying these options.

30 Troubleshoot Enterprise

Troubleshooting the Enterprise appliance

For information about troubleshooting the Marketplace Portal and Cloud Service Management Console, see the *HP CSA Documentation List* at Enterprise Information Library.

Enterprise cannot communicate with Foundation after the Foundation network configuration is changed

Symptom	Possible cause and recommendation
• You cannot create subscriptions in the Marketplace Portal • You cannot create designs or edit existing designs in HP CSA • You cannot manage existing subscriptions in HP CSA	**Foundation network settings were changed** If the Foundation appliance host name, IP address, subnet mask, gateway address, DNS server or alternate DNS server is changed after Enterprise is installed, the Enterprise appliance can no longer communicate with the Foundation appliance • Manage existing Enterprise subscriptions in the CloudSystem Portal, or • Reset your environment by uninstalling, then reinstalling Enterprise from the Enterprise screen in the CloudSystem Console. **NOTE:** Uninstalling Enterprise deletes all subscriptions created in HP CSA.

Cannot see Enterprise installation progress

Symptom	Possible cause and recommendation
You cannot see the Enterprise installation progress indicator	**You terminated your console session** 1. While the installation is in progress, keep your console session active. • Do not refresh the **Enterprise** screen. • Do not log off the CloudSystem console. **NOTE:** While the installation is in progress, you can navigate to other console screens and see the progress indicator when you return to the **Enterprise** screen.

Cannot create a design in HP CSA

Symptom	Possible cause and recommendation
When you attempt to create a design in HP CSA, images and flavor resources are not displayed	**The Foundation and Enterprise management hypervisor hosts have different time settings** 1. Uninstall the Enterprise appliance. 2. Log on to the management hypervisor hosting the Enterprise appliance. 3. Set the time to sync with an NTP server. 4. Reinstall the Enterprise appliance.

Cannot provision a design with server groups connected to more than one volume group on ESX compute nodes

Symptom	Possible cause and recommendation
Provisioning does not succeed	**Limitation in CloudSystem Enterprise** 1. Create a design with server group(s) connected to one volume group. 2. Retry the provision operation.

Cannot create a subscription with a volume group attached to a server group

Symptom	Possible cause and recommendation
When trying to create a subscrioption with a volume group attached to a server group, the subscription does not succeed and the volume is not attached	**The template does not contain enough volumes for each of the servers** • Create a design in which the number of instances defined in the volume group attached to a server group matches the number of instances in the server group. **The device parameter has invalid data** • Ensure that the device parameter as defined in the design for each volume is correctly set. Examples of invalid data for a device parameter are `/de/fddd` and `/dev/fddd`.

Volumes are not presented when attaching a volume to a design

Symptom	Possible cause and recommendation
When you attemp to attach a volume to a design in the Topology Designer, not all volumes are presented	**Volumes created by an administrator are not presented to a user creating a topology** • Select from the volumes presented, or • Ask the administrator to attach the volume to the topology.

Adding a server to a server group does not delete partially provisioned servers

Symptom	Possible cause and recommendation
The Add server to group operation did not succeed but one or more new servers was provisioned and added to the server group	**The hypervisor does not have enough resources to complete the operation, the image is no longer available, or communication issues occurred between Enterprise and Foundation** • Use the Remove server from server group operation to remove the new servers from the server group, then try the operation again.

HP CSA does not clean up resources when a subscription does not succeed

Symptom	Possible cause and recommendation
The resources created during the subscription process are not cleaned up	**The subscription cannot attach a volume and does not complete** • Manually delete the volume and server resources in the CloudSystem Console.

Cannot create a subscription configured to create a new router

Symptom	Possible cause and recommendation
When you attempt to create a new subscription that creates a new router, the operation does not succeed	**The network already has an associated router** The router may have been created when a subscription based on the same template was previously created, or the the router was created manually in the CloudSystem Portal. • Edit the template to use the existing router, then try the operation again.

Cannot create a template without a keypair

Symptom	Possible cause and recommendation
You copied an existing topology that does not contain a keypair, but you cannot create a template from the topology	**A topology to be used as a template requires a keypair** • Provide a keypair for the topology, then try creating the template again.

Removing a volume group from a subscription does not succeed

Symptom	Possible cause and recommendation
You see `Service Instance Status: Modification Failed`	**You selected "Remove An Attached Volume Group" from a deployed service that was created with more than one volume group** • Do not attempt to remove an attached volume group from a service.

Some Cloud OS endpoints are visible but are not supported APIs for use by external clients

Symptom	Possible cause and recommendation
You see these Cloud OS endpoints in the CloudSystem Portal: • **Infrastructure Topology Provisioning Service (Eve)** • **Resource Pool Registry and Capability Tagging Service (Graffiti)** • **Topology Design Registry and Repository Service (Focus)**	**APIs are internal and are intended to be used only by the Enterprise system** • Do not attempt to use these APIs. There is no external IP address. The Cloud OS endpoints are registered in the OpenStack Identity Service (Keystone) catalog, and may be visible in the CloudSystem Portal but they are not supported APIs for use by external clients.

Part VII Appendices

A Enabling strong certificate validation in the CloudSystem Portal

This appendix describes how to configure the CloudSystem Portal to enable strong SSL/TLS validation. Strong validation means that the LDAP server requires a valid client CA certificate chain when an OpenLDAP or Microsoft Active Directory service is used for authentication.

To enable strong certificate validation in the CloudSystem Portal, you will:

- Export the certificate chain from the directory server
- Import the certificate chain to the CloudSystem Foundation base appliance through the hypervisor management console

Follow the instructions for the directory service you have configured for authentication. For more information, see Configuring CloudSystem to use Active Directory or OpenLDAP directory authentication (page 55).

Enabling strong certificate validation if your directory service is OpenLDAP (page 189)
Enabling strong certificate validation if your directory service is Active Directory (page 190)

Prerequisites

- The OpenLDAP or Active Directory server certificate contains a Fully Qualified Domain name (FQDN) in the CN attribute Subject field.
- The FQDN of the OpenLDAP or Active Directory server is resolvable by the CloudSystem Foundation base appliance.

  To verify that the FQDN is resolvable:

  1. Log in to the CloudSystem Foundation base appliance console and run the following command.

     ```
     nslookup <directory-server-FQDN>
     ```

     See Enable console access and set the password (page 199).
  2. If an IP address is returned, continue to Enabling strong certificate validation if your directory service is OpenLDAP (page 189) or Enabling strong certificate validation if your directory service is Active Directory (page 190).
  3. If an IP address is *not* returned, update the CloudSystem Foundation network configuration to include the IP address of an alternate DNS server that resolves the LDAP or Active Director server name as an IP address.

  IMPORTANT: If CloudSystem Enterprise is installed, changing the network configuration of the CloudSystem Foundation base appliance in the following steps requires that you uninstall, then reinstall Enterprise. See Before installing Enterprise (page 126).

     a. From the main menu in the CloudSystem Console, select **Settings**.
     b. Click the **Edit** icon in the Appliance panel.
     c. Expand Network 1 (Appliance).
     d. In the **Alternate DNS server** box, enter the **IP address** of a DNS server that resolves the OpenLDAP or Active Directory server.

Using OpenLDAP

Procedure 83 Enabling strong certificate validation if your directory service is OpenLDAP

1. Log in to the CloudSystem Foundation base appliance console. See Enable console access and set the password (page 199).
2. Get the entire LDAP server certificate chain.

   ```
   sudo openssl s_client -showcerts -host <directory-server-FQDN> -port
   636 > ldapserver.pem
   ```

NOTE: If you are using a load-balanced (round robin) solution for your directory server, obtain the FQDN of one node in the server by entering the following commands.

```
nslookup <directory-server-FQDN>
```

A list of IP addresses is returned. Select one IP address and enter:

```
nslookup <directory-server-IP address>
```

Enter the FQDN returned for this IP address as the *<directory-server-FQDN>* in the `openssl` command above.

3. Edit `ldapserver.pem` and remove all lines except for the contents of the certificate, and the **Begin Certificate** and **End Certificate** lines.

   Keep all certificates in the file so that you include the entire chain. If your certificate chain has more than one CA, all CAs must be included. Make sure there are no blank lines or white space.

   Example `ldapserver.pem` file after editing:

   ```
   -----BEGIN CERTIFICATE-----
   M123DTCCAvWgAwIBAgIJANgTCE…
   IFl1P+c9Gro82S7z
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   MIIEDTCCAvWgAwIBAgIJANgTCE…
   IFl1P+c9Gro82S7z
   -----END CERTIFICATE-----
   ```

4. Replace the old `ldapserver.pem` certificate file with the new file using the following commands:

   ```
   sudo mv /ci/data/keystone/ldapserver.pem /ci/data/keystone/ldapserver.pem.old
   sudo mv ldapserver.pem /ci/data/keystone/ldapserver.pem
   sudo chown trm1:keystone /ci/data/keystone/ldapserver.pem
   sudo chmod 640 /ci/data/keystone/ldapserver.pem
   ```

5. Edit `/etc/keystone/keystone.conf` and delete the line `tls_req_cert = allow`.

   ```
   sudo sed -i "s/tls_req_cert = allow//g" /etc/keystone/keystone.conf
   ```

6. Restart the OpenStack-Keystone service.

   ```
   sudo service openstack-keystone restart
   ```

Using Active Directory

Procedure 84 Enabling strong certificate validation if your directory service is Active Directory

1. Export the Certificate Authority (CA) certificate to a file by entering the following command where Active Directory Certificate Services is running:

   ```
   certutil -ca.cert CA.cer > ca.pem
   ```

2. Copy the `ca.pem` file to an internal Secure FTP (SFTP) server. Use TEXT as the transfer mode.
3. Log in to the CloudSystem Foundation base appliance console. See Using the CloudSystem appliances console (page 199).
4. Get the exported `ca.pem` file from the internal SFTP server.
5. Get the Active Directory server certificate.

   ```
   sudo openssl s_client -showcerts -host <directory-server-FQDN> -port
   636 > ad.pem
   ```

NOTE: If you are using a load-balanced (round robin) solution for your directory server, obtain the FQDN of one node in the server by entering the following commands.

`nslookup <directory-server-FQDN>`

A list of IP addresses is returned. Select one IP address and enter:

`nslookup <directory-server-IP address>`

Enter the FQDN returned for this IP address as the `<directory-server-FQDN>` in the `openssl` command above.

6. Edit `ad.pem` and remove all lines except for the contents of the certificate, and the **Begin Certificate** and **End Certificate** lines.

   Keep all certificates in the file so that you include the entire chain. Make sure there are no blank lines or white space.

   Example `ad.pem` file after editing:

   ```
   -----BEGIN CERTIFICATE-----
   MIIEDTCCAvWgAwIBAgIJANgTCE
   …
   IFl1P+c9Gro82S7z
   -----END CERTIFICATE-----
   ```

7. Join the `ca.pem` and `ad.pem` certificates into `ldapserver.pem` by entering the following command.

   ```
   sudo cat ca.pem ad.pem > ldapserver.pem
   ```

8. Replace the old `ldapserver.pem` certificate file with the new file using the following commands:

   ```
   sudo mv /ci/data/keystone/ldapserver.pem /ci/data/keystone/ldapserver.pem.old
   sudo mv ldapserver.pem /ci/data/keystone/ldapserver.pem
   sudo chown trm1:keystone /ci/data/keystone/ldapserver.pem
   sudo chmod 640 /ci/data/keystone/ldapserver.pem
   ```

9. Edit `/etc/keystone/keystone.conf` and delete the line `tls_req_cert = allow`.

   ```
   sudo sed -i "s/tls_req_cert = allow//g" /etc/keystone/keystone.conf
   ```

10. Restart the OpenStack-Keystone service.

    ```
    sudo service openstack-keystone restart
    ```

B Working with the csadmin CLI

The csadmin CLI provides command line access for storage system administrative tasks, private network VLAN management tasks, appliance management tasks, and console user management tasks.

This appendix provides information on how to configure a CLI shell to ease secure access when using the csadmin command line and how to view available help from the command line. It defines required and optional csadmin command syntax, and provides usage examples.

The csadmin CLI provides command line access for storage system administrative tasks, private network VLAN management tasks, appliance management tasks, and console user management tasks.

NOTE: See Supported console operations on the CloudSystem appliances (page 199) for information about using csadmin to enable access to the CloudSystem Foundation and CloudSystem Enterprise appliance consoles from the hypervisor console and setting a password for the cloudadmin user.

Configure a CLI shell to ease secure access when using csadmin

Configuring a CLI shell enables you to automatically apply permissions to commands rather than entering the full CLI syntax with all permissions each time you run a command.

Procedure 85 Configuring a CLI shell

1. On a Windows or Linux system where csadmin is installed, open a command shell.
2. Configure a shell to identify command permissions by entering commands similar to the following. For example, if you are using a Linux system, enter:

   ```
   export OS_USERNAME=<admin_user_name>export OS_PASSWORD=<admin_password>
   export OS_AUTH_URL=https://<IP_address_of_base_appliance>/rest/identity/v2.0
   ```

   If you are using a POSIX shell on a Windows system, enter:

   ```
   set OS_USERNAME=<admin_user_name>
   set OS_PASSWORD=<admin_password>
   set;
   OS_AUTH_URL=https://<IP_address_of_base_appliance>/rest/identity/v2.0
   ```

See also Troubleshoot csadmin (page 183).

Getting help for csadmin

To view csadmin help from the command line, use either of the following commands.

- `csadmin --help`

  Lists all available CLI commands and additional details for optional arguments.

- `csadmin help <command name>`

  Lists detailed help for a specific command.

Order of syntax for commands and arguments

The following example shows the order of syntax for all csadmin CLI commands and arguments.

```
csadmin <optional arguments> <cmd> <required common arguments for the command> <optional common arguments for
the command> <args specific to the command> <positional argument for the command>
```

Optional arguments

You can enter the following optional arguments directly after the csadmin command.

- `--version`: Shows the program version number and exits the csadmin CLI.
- `-v, --verbose`: Increases the amount of output displayed. This command can be repeated.

- `--log-file LOG_FILE`: Specifies a log file for storing output. By default, this is disabled.
- `-q, --quiet`: Restricts display output to warnings and error messages.
- `-h, --help`: Shows the help message and exits the `csadmin` CLI.
- `--debug`: Shows trace back information to help debug errors.

Required common arguments

- `--os-auth-url <auth-url>`: Specifies the OpenStack Identity Service endpoint to use for authentication. Defaults to `-OS_AUTH_URL`.
- `--os-username <auth-username>`: Specifies a user name to use for OpenStack Identity Service authentication. Defaults to `OS_USERNAME`.
- `--os-password <auth-password>`: Specifies a user password to be used for OpenStack Identity Service authentication. Defaults to `OS_PASSWORD`.

Optional common arguments

- `--os-tenant-name <auth-tenant-name>`: Specifies a private network name for which to request authorization. Defaults to `OS_TENANT_NAME`.
- `--os-tenant-id <auth-tenant-id>`: Specifies the ID of a tenant requesting authorization. Defaults to `OS_TENANT_ID`.
- `--os-region-name <auth-region-name>`: Specifies a region name used for authentication. Defaults to `OS_REGION_NAME`.
- `--os-cert <cert>`: Not supported.
- `--os-hp-cs-api-version <hp-cs-api-version>`: Not supported.
- `–os-cacert<cert>`: Specifies the CA certificate bundle to use to validate the server certificate. Defaults to `OS_CACERT`. See Certificate verification errors (page 183).
- `--os-key <key>`: Not supported.
- `--insecure`: Does not verify the certificate chain on the server. Defaults to “false” or `OS_INSECURE`. See Certificate verification errors (page 183).
- `–h, --help`: Shows the help message and exits the `csadmin` CLI.

Command syntax and examples

- **appliance list**: Lists auxiliary virtual machines.

```
csadmin appliance list <required and/or optional common args> <args specific to the command>
```

Examples

```
csadmin appliance list --os-username adminuser --os-password adminpassword --os-auth-url
10.x.x.x –insecure
```

```
csadmin appliance list --long --os-username adminuser --os-password adminpassword --os-auth-url
 10.x.x.x --insecure
```

```
csadmin appliance list --va esx_iscapp01 --long --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x --insecure
```

Arguments	Definition
`-;l, --long`	Displays information in a long listing format.
`--va <VM name>`	The unique name of the appliance.

- **appliance support-dump**: Handles the support dump of an auxiliary virtual machine.

```
csadmin appliance support-dump  <required and/or optional common args> <args specific to the command>
```

Examples

```
csadmin appliance support-dump --list --os-username adminuser --os-password adminpassword
--os-auth-url 10.x.x.x –insecure
```

```
csadmin appliance support-dump --va esx_iscapp01 --file esx_iscapp01.dump --os-username
adminuser --os-password adminpassword --os-auth-url 10.x.x.x –insecure
```

Arguments	Definition
`--va <VM name>`	The unique name of the appliance from which to take the support dump. Run `csadmin appliance support-dump --list` to get the appliance names.
`--file <output file name>`	The output file where the support dump is copied.
`--list`	Lists the auxiliary virtual machines capable of producing support dumps.

- **block-storage-driver create**: Creates a block storage driver.

```
csadmin block-storage-driver create <required and/or optional common args> <args specific to the
command><name of new block storage driver>
```

Example

```
csadmin block-storage-driver create --attributes
"hp3par_username:3paradm  hp3par_password:3pardata
 hp3par_api_url:https://10.x.x.x:8080/api/v1  virtualDomain:-hp3par_cpg:FC_r6"
--drivertype 3PAR-FC  --os-username adminuser --os-password adminpassword
--os-auth-url 10.x.x.x --insecure FCDriver
```

NOTE: Entering a dash (–) after `virtualDomain:`, as shown in the example, specifies the default virtual domain.

Arguments	Definition
`--description <description>`	An optional description for the storage driver.
`--drivertype <Driver Type>`	Driver type for the storage driver, such as 3PAR-FC, or 3PAR-ISCSI.
`--attributes <attributes>`	Driver-specific attributes in the format of `"key 1:value1 key2:value2....."` For example, to create a storage driver with the 3PAR-FC or 3PAR-ISCSI driver type, enter: `--attributes "hp3par_username:3paradm hp3par_password:myPassword hp3par_api_url:https://10.x.x.x:8080/api/v1 virtualDomain:myDomain hp3par_cpg:myCpg"`

- **block-storage-driver delete**: Deletes a block storage driver.

```
csadmin block—storage—driver delete <required and/or optional common args> <name of new block storage
driver to delete>
```

Example

```
csadmin block-storage-driver delete --os-username adminuser --os-password adminpassword
--os-auth-url 10.x.x.x --insecure FCDriver
```

- **block-storage-driver list**: Lists block storage drivers.

```
csadmin block—storage—driver list <required and/or optional common args>
```

Example

```
 csadmin block-storage-driver list --os-username adminuser--os-password adminpassword
--os-auth-url 10.x.x.x --insecure
```

- **block-storage-driver show**: Shows a single block storage driver.

```
csadmin block—storage—driver show <required and/or optional common args> <name of new block storage driver
 to show>
```

Example

```
 csadmin block-storage-driver show --os-username adminuser --os-password adminpassword
--os-auth-url 10.x.x.x --insecure FCDriver
```

- **block-storage-driver update**: Updates a block storage driver.

```
csadmin block-storage-driver update <required and/or optional common args> <args specific to the command>
 <name of block storage driver to update>
```

Example

```
csadmin block-storage-driver update --attributes "hp3par_username:3paradm
hp3par_password:3pardata  hp3par_api_url:https://16.124.134.19:8080/api/v1  virtualDomain:- hp3par_cpg:FC_r1"
--os-username adminuser  --os-password adminpassword --os-auth-url 10.x.x.x --insecure  FCDriver
```

Arguments	Definition
`--newname <newname>`	Name to replace existing storage driver name.
`--description <description>`	Description for the storage driver.
`--attributes <attributes>`	Driver-specific attributes in the format of `"key 1:value1 key2:value2....."` For example, to create a storage driver with the 3PAR-FC or 3PAR-ISCSI driver type, enter: `--attributes "hp3par_username:3paradm hp3par_password:myPassword hp3par_api_url:https://10.x.x.x:8080/api/v1 virtualDomain:myDomain hp3par_cpg:myCpg"`

- **block-storage-driver-type create**: Creates a block storage driver type. The driver type is used to create a block storage driver. It defines the volume driver metadata.

```
csadmin block-storage-driver-type create <required and/or optional common args> <args specific to the
command><name of new storage system>
```

Example

```
csadmin block-storage-driver-type create --description "vmware driver" --volume-driver
cinder.volume.drivers.vmware.vmdk.VMwareVcVmdkDriver --attributes "vmware_host_ip
vmware_host_username vmware_host_password" --insecure --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x VMwareVcVmdkDriver
```

Arguments	Definition
`--volume-driver <volume driver>`	Volume driver of the block storage driver. For example, `cinder.volume.drivers.san.hp.hp_3par_fc.HP3PARFCDriver`
`--attributes <attributes>`	Block storage driver type attributes in the format of `"key 1:value1 key2:value2....."`
`--description <description>`	Description of the block storage driver type.

- **block-storage-driver-type delete**: Deletes a block storage driver type.

```
csadmin block-storage-driver-type delete <required and/or optional common args> <args specific to the
command><name of the block storage driver to be deleted>
```

Example

```
csadmin block-storage-driver-type delete --insecure --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x VMwareVcVmdkDriver
```

- **block-storage-driver-type list**: Lists the block storage driver types.

```
csadmin block—storage-driver-type list <required and/or optional common args> <args specific to the command>
```

Example

```
csadmin block-storage-driver-type list --insecure --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x
```

- **block-storage-driver-type show**: Shows block storage drive type details.

```
csadmin block—storage—driver-type show <required and/or optional common args> <name of new block storage
 driver type to show>
```

Example

```
csadmin block-storage-driver-type show --insecure --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x VMwareVcVmdkDriver
```

- **block-storage-driver-type update**: Updates a block storage driver type.

```
csadmin block-storage-driver-type update <required and/or optional common args> <args specific to the
command> <name of block storage driver type to update>
```

Example

```
csadmin block-storage-driver-type update --description "vmware driver updated" --volume-driver
 cinder.volume.drivers.vmware.vmdk.VMwareVcVmdkDriver --attributes "vmware_host_ip
vmware_host_username vmware_host_password" --insecure --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x VMwareVcVmdkDriver
```

Arguments	Definition
`--newname <newname>`	Name to replace existing block storage driver type name.
`--description <description>`	Description for the block storage driver type.
`--volume-driver <volume driver>`	Volume driver of the block storage driver. For example, `cinder.volume.drivers.san.hp.hp_3par_fc.HP3PARFCDriver`
`--attributes <attributes>`	Block storage driver type attributes in the format of `"key 1:value1 key2:value2....."`

- **volume-type create**: Creates a Cinder volume type.

```
csadmin volume—type create <required and/or optional common args> <args specific to the command> <name of
 the volume type to create>
```

Example

```
csadmin volume-type create --driver-name FCDriver --attributes "cpg:myCPG  host-mode:VMware
allocation-type:thin" --os-username adminuser --os-password adminpassword --os-auth-url 10.x.x.x
 --insecure volume-type-fc
```

Arguments	Definition
`--driver-name <name of the block storage driver>`	The name of the block storage driver on which to base the CVT and driver configuration. Run `block storage-driver list` to get the list.-
`--attributes <attributes>`	Volume type-specific attributes in the format of `"key 1:value1 key2:value2....."` For example, to create a volume type with a 3PAR driver instance, enter: `--attributes "cpg:myCpg hoste mode:VMware allocation type:thin"`
`--description <description>`	An optional description of the volume type.

- **volume-type delete**: Delete Cinder volume types.

```
csadmin volume—type delete <required and/or optional common args> <name of the volume type to delete>
```

Example

```
csadmin volume-type delete --os-username adminuser --os-password adminpassword --os-auth-url
10.x.x.x --insecure volume-type-FC
```

- **volume-type list**: Lists Cinder volume types.

```
csadmin volume—type list <required and/or optional common args>
```

Example

```
csadmin.exe volume-type list --os-username adminuser --os-password adminpassword --os-auth-url
 10.x.x.x --insecure
```

- **volume-type show**: Shows information about a single Cinder volume type.

```
csadmin volume—type show <required and/or optional common args> <name of the volume type>
```

Example

```
csadmin volume-type show --os-username adminuser --os-password adminpassword --os-auth-url
10.x.x.x --insecure volume-type-FC
```

- **volume-type update**: Updates a Cinder volume type.

```
csadmin volume—type update <required and/or optional common args> <args specific to the command> <name of
 the volume type to update>
```

Example

```
csadmin volume-type update --attributes
"cpg:myCPG  host-mode:VMware   allocation-type:thin" --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x --insecure volume-type-FC
```

Arguments	Definition
`--driver-name <name of the block storage driver>`	The name of the block storage driver on which to base the CVT and driver configuration. Run `block storage-driver list` to get the list.
`--attributes <attributes>`	Volume type-specific attributes in the format of `"key 1:value1 key2:value2....."` For example, to create a volume type with a 3PAR driver instance, enter: `--attributes "cpg:myCpg hoste mode:VMware allocation type:thin"`
`--description <description>`	An optional description of the volume type

- **console-users disable**: Disables cloud administrator user access.

```
csadmin console-users disable  <required and/or optional common args> <args specific to the command>
```

Example

```
csadmin console-users disable --vm-name esx_iscapp01 --os-username adminuser --os-password
adminpassword --os-auth-url 10.0.0.1 --insecure
```

Argument	Definition
`--vm <VM name>`	The CloudSystem appliance to be accessed by the cloud administrator user from a hypervisor console. This name is set in `csstart` or in the Foundation console during first time setup.

- **console-users enable**: Enables cloud administrator users. See Enable console access and set the password (page 199).
- **console-users getInfo**: Lists cloud administrator user details.

```
csadmin console-users getInfo  <required and/or optional common args> <args specific to the command>
```

Example

```
csadmin console-users getInfo --vm-name esx_iscapp01 --os-username adminuser --os-password
adminpassword --os-auth-url 10.x.x.x --insecure
```

Argument	Definition
`--vm <VM name>`	The CloudSystem appliance to be accessed by the cloud administrator user from a hypervisor console. This name is set in `csstart` or in the Foundation console during first time setup.

- **console-users set-password**: Sets the cloud administrator user password. See Enable console access and set the password (page 199).
- **tenant-vlan add**: Adds the specified VLAN IDs to the range of VLANs available to private networks.

```
csadmin tenant—vlan add <required and/or optional common args> <args specific to the command> <a VLAN ID,
 an integer 1-4096>
```

Example

```
csadmin tenant-vlan add 10 12 14 15 --range start=20,end=25 --range start=30,end=40 --os-username
 adminuser --os-password adminpassword --os-auth-url 10.x.x.x —insecure
```

Argument	Definition
`--range start=<vlan-id>, end=<vlan-id>`	A VLAN range in the form `start=N,end=N+M`.

- **tenant-vlan delete**: Deletes the specified VLAN IDs from the range of VLANs available to private networks.

  ```
  csadmin tenant—vlan delete <required and/or optional common args> <args specific to the command>
  <a VLAN ID, an integer 1-4096>
  ```

  Example

  ```
  csadmin tenant-vlan delete --range start=21,end=23 12 1
  ```

Argument	Definition
`--range start=<vlan-id>, end=<vlan-id>`	A VLAN range in the form start=N,end=N+M.

- **tenant-vlan list**: Lists private network VLAN IDs.

  ```
  csadmin storage—system list <required and/or optional common args>
  ```

  Example

  ```
  csadmin tenant-vlan list --os-username adminuser --os-password adminpassword --os-auth-url
  10.x.x.x —insecure
  ```

C Supported console operations on the CloudSystem appliances

CloudSystem provides a command line interface accessible from the management hypervisor console underlying the Foundation base appliance, Enterprise appliance, and vCenter Server proxy appliance. You can use the hypervisor console to access the appliance console to perform the supported tasks listed in CloudSystem appliance console tasks (page 200).

Enable console access and set the password

Use the following `csadmin console-users` CLI commands to enable console access for cloud administrator users and to set the password. The `csadmin console-users` commands are supported on the CloudSystem Foundation base appliance, the Enterprise appliance, and the proxy appliances.

Procedure 86 Enabling console access

This command enables access to the console of the specified appliance.

1. On a Windows or Linux system where `csadmin` is run, open a command shell.
2. Enter the following command:

   ```
   csadmin console-users enable --vm-name  <VM name>
   ```

   `<VM name>`—Name of the CloudSystem appliance to be accessed by the cloud administrator user from a hypervisor console. This name is set in `csstart` or in the Foundation console during first time setup.

   Example

   ```
   csadmin console-users enable --vm-name esx_iscapp01 --os-username adminuser --os-password adminpassword
   --os-auth-url 192.0.0.1 --insecure
   ```

Procedure 87 Setting the password for console access

This command sets the password for the cloud administrator user (`cloudadmin`) on the specified appliance. You can set a different password for each appliance on which you enabled access.

1. On the `csadmin` command line, enter the following command:

   ```
   csadmin console-users set-password --password <password> --vm-name <VM name>
   ```

   - `<password>`—Password for `cloudadmin` on the specified appliance.
   - `<VM name>`—Name of the CloudSystem appliance to be accessed by the cloud administrator user from a hypervisor console. This name is set in `csstart` or in the Foundation console during first time setup.

   Example

   ```
   csadmin console-users set-password --vm-name esx_iscapp01 --password password --os-username adminuser
   --os-password adminpassword --os-auth-url 192.0.0.1 --insecure
   ```

2. To shorten command syntax by automatically applying command permissions, see Configure a CLI shell to ease secure access when using csadmin (page 192).

Using the CloudSystem appliances console

This section describes how to use the hypervisor console to access the appliance consoles and perform supported actions.

Logging in to the appliance consoles

After the console is enabled for a given appliance and you have access to the appliance console, you can log in to the appliance by specifying the `cloudadmin` user name and the password set in the `csadmin console-users set-password` command. Make sure you have set a password for the appliance you are trying to access.

Procedure 88 Logging in to the appliance consoles

1. From the management hypervisor, select the **Console** tab.

2. Access the appliance console login screen that you enabled in Enabling console access by pressing **Alt-Ctl-F1**.
3. Log in to the appliance console with the following credentials:

   User name: `cloudadmin`

   Password: *<Password>* that you set for the appliance in Setting the password for console access.

Procedure 89 Switching between the hypervisor console and the CloudSystem UI

From the management hypervisor console, you can use keystrokes to switch to the CloudSystem UI running in the hypervisor console, and back to the appliance console.

1. From the management hypervisor, select the **Console** tab.
2. To access the appliance console login screen, press **Alt-Ctl-F1**.
3. To switch to the CloudSystem UI running in the console, press **Alt-F2**.

CloudSystem appliance console tasks

The following table describes supported tasks you can perform using the CloudSystem appliance console running in the management hypervisor console.

NOTE: Administrators who make any other changes to the state of the appliances do so at their own risk. If you encounter issues after making unsupported changes, HP may require you to reproduce the issue with an unmodified appliance before offering support.

Table 14 CloudSystem CLI console tasks

Task	Procedure

Enable vCenter Server and vShield certificate validation	You must complete the following steps before you register the VMware vCenter Server on the Integrated Tools screen.
	1. Access the CloudSystem Foundation appliance console from the management hypervisor console and log in as `cloudadmin`.
	2. Open the file.
	`/etc/isc-esxproxy-management-service/isc-esxproxy-management-service-api.conf`
	3. Locate the `vmware_cert_check` setting and change the value from `false` to `true`.
	4. Save the file.
	5. Restart the ESX proxy management service.
	`#service isc-esxproxy-management-service restart`

Enable strong certificate validation in the CloudSystem Portal	The operations in Enabling strong certificate validation in the CloudSystem Portal (page 189) are supported in the CloudSystem Foundation appliance console.

Import the LDAP certificate to the HP CSA keystore so that HP CSA con be configured to communicate with the LDAP server using SSL.	This operation is used to configure the Enterprise appliance to integrate with LDAP using SSL. This operation is necessary when Enterprise is configured for multitenancy or when adding users from LDAP.
	1. Access the CloudSystem Enterprise appliance console from the management hypervisor console and log in as `cloudadmin`.
	2. Create the certificate file based on the LDAP certificate server configuration.
	`sudo echo -n | openssl s_client -connect <LDAP_server_host>:<LDAP_server_port>| sed -ne '/BEGIN CERTIFICATE/,/END CERTIFICATE/p' > ldapserver.cer`
	where *LDAP_server_host* is either the IP address or the host name, depending on how the server was configured.
	3. Import the certificate into the HP CSA Java Keystore (`csa/openjre/lib/security/cacerts`).
	`sudo sh -c 'keytool -import -alias ldap_certificate -file /ci/etc/cloudadmin/ldapserver.cer -keystore /ci/usr/local/hp/csa/openjre/lib/security/cacerts -storepass changeit'`
	4. Restart the CSA service and the Marketplace Portal service.

Table 14 CloudSystem CLI console tasks *(continued)*

Task	Procedure

	`sudo sh -c 'service csa restart'`
	`sudo sh -c 'service mpp restart'`
	5. Switch to the HP CSA console.
	6. Enable the SSL option.
	7. Change the port number to the LDAP server SSL port number you specified in step 2.

Configure HP CSA to allow CloudSystem Enterprise to connect to HP Matrix Operating Environment (Matrix OE), CloudSystem Foundation, and HP Operations Orchestration (OO) Central	The operations in Appendix B, "Configuring additional providers for CloudSystem Enterprise" in the *HP CloudSystem Installation and Configuration Guide* at Enterprise Information Library are supported in the CloudSystem Enterprise and CloudSystem Foundation appliance consoles.

Configure the CloudSystem Enterprise appliance to use the NTP server(s) configured for the ESX hosts	If CloudSystem Enterprise is deployed on ESX, configure the Enterprise appliances to synchronize with the NTP servers configured for the ESX hosts.
	If CloudSystem Enterprise is deployed on KVM, this operation is not required.
	1. Access the CloudSystem Enterprise appliance console from the management hypervisor console and log in as `cloudadmin`.
	2. Edit the NTP configuration file to add the NTP server entries.
	`sudo vi/etc/ntp.conf`
	3. Restart the NTP service.
	`sudo service ntpd restart`

Configure the CloudSystem Enterprise appliance to support parallel subscription requests through CloudSystem Foundation and subscriptions with a large number of resources	**1.** Access the CloudSystem Enterprise appliance console from the management hypervisor console and log in as `cloudadmin`.
	2. Edit the [workflow] section in the file `/etc/eve-requestworker/eve.yml` to set the following values.
	`[workflow]`
	`maxNumberConcurrentJobs: 10`
	`maxNumberThreadsPerJob: 5`
	`maxNumberTotalThreads: 25`
	`submissionTimeout: 7200`
	3. Restart the eve-api and eve-requestworker services by entering:
	`# service eve-api restart`
	`# service eve-requestworker restart`
	Values are:
	• `maxNumberConcurrentJobs`: Maximum number of concurrent create/delete subscriptions and lifecycle operations. Concurrent operations that exceed this number will be queued.
	• `maxNumberThreadsPerJob`: Maximum number of threads per job in the Enterprise appliance.
	• `maxNumberTotalThreads`: Maximum number of Foundation calls that Enterprise will trigger (create/delete instance, create/delete/attach/detach volume, create router, and so on).
	• `submissionTimeout`: Maximum time to wait for a response before changing the status of the subscription or lifecycle operation to failed.

Change the default passwords for the HP CSA admin and consumer users in CloudSystem Enterprise	The operations in Logging in and changing the default HP CSA and Marketplace Portal password (page 128) are supported in the CloudSystem Enterprise appliance console.
Change the password of the management vCenter Server hypervisor in the `/etc/pavmms/deployer.conf` file	**1.** Access the CloudSystem Foundation appliance console from the management hypervisor console and log in as `cloudadmin`. **2.** Open the `deployer.conf` file. Use `sudo su` if you need elevated privileges access. **3.** Locate the `Hypervisor` section of the file.

Table 14 CloudSystem CLI console tasks *(continued)*

Task	Procedure
	4. Change the `username` and the `password` values. **5.** Save the file.
Change the image file locations in the `/etc/pavmms/deployer.conf` file	**1.** Access the CloudSystem Foundation appliance console from the management hypervisor console and log in as `cloudadmin`. **2.** Open the `deployer.conf` file. Use `sudo su` if you need elevated privileges access. **3.** Locate the `Images` section of the file. **4.** Change the values for the image locations. For KVM, enter an absolute path to your directory and image file. For ESXi, enter the name of your template VM without any path components. • `base-image`—Base appliance image file or template name • `SDN-image`—SDN appliance image file or template name • `net-node-image`—Network node appliance image file or template name • `net-node-image`—Network node appliance image file or template name • `proxy-image`—(Optional) ESX proxy image file or template name • `advanced-image`—(Optional) Advanced appliance image file or template name **5.** Save the file.

Customize the Cloud Service Management Console (HP CSA)	**1.** Access the CloudSystem Foundation appliance console from the management hypervisor console and log in as `cloudadmin`.
	2. Back up the HP CSA configuration files.
	`sudo cp -p /ci/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/deployments/csa.war/dashboard/config.json /ci/etc/cloudadmin`
	`sudo cp -p /ci/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/deployments/csa.war/custom/messages.properties /ci/etc/cloudadmin`
	3. Open the HP CSA dashboard configuration file for editing.
	`sudo vim /ci/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/deployments/csa.war/dashboard/config.json`
	4. Enable custom features. For example, enable the "provider panel" on the CSA dashboard.
	a. Search the file for the `providerpanel id` section.
	b. Change the `enabled` value to `true`.
	c. Save the file.
	d. Reload the HP CSA console UI.
	More options are listed in the HP CSA dashboard configuration file.
	5. Continue customizing HP CSA dashboard features. For example:
	• Enable a URL link in the dashboard.
	a. Reopen the HP CSA dashboard file for editing. (See step 3).
	b. Search the file for the `custom id` section.
	c. Change the `enabled` value to `true`.
	d. Change the `data` value to any valid URL.
	e. Change the `target` value to `new`.
	f. Save the file.
	g. Reload the HP CSA console UI.
	The new URL link appears on the HP CSA dashboard.
	To restore the default HP CSA configuration files, enter:
	`sudo cp -p /ci/etc/cloudadmin/config.json /ci/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/deployments/csa.war/dashboard`

Table 14 CloudSystem CLI console tasks *(continued)*

Task	Procedure
	`sudo cp -p /ci/etc/cloudadmin/messages.properties /ci/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/deployments/csa.war/custom`

Perform post-restore resynchronization tasks on the CloudSystem Foundation appliance	**1.** Access the CloudSystem Foundation appliance console from the management hypervisor console and log in as `cloudadmin`.
	2. Enter this command to start the synchronization process. Use `sudo su` if you need elevated privileges access.
	`service iscrecovery resync`
	3. Check the Activity log for the following Alert:
	`The system is ready for use.`
	`Resynchronization will continue for a period of 24 hours as resources come on line.`
	`Initial synchronization of CloudSystem with the environment is complete.`
	For more information about restore actions, see the *HP CloudSystem Foundation and Enterprise Software: Recommended backup and restore procedures* at Enterprise Information Library.

D Limitations on support for OpenStack CLI commands

The following tables list CLI commands for OpenStack modules that are not supported in HP CloudSystem.

For a list of all OpenStack Havana CLI commands, see *OpenStack Documention for Havava releases*.

Table 15 Unsupported Keystone commands

Command	Task
`discover`	Discover Keystone servers, supported API versions, and extensions.
`ec2-credentials-create`	Create EC2-compatible credentials for user per tenant (private network).
`ec2-credentials-delete`	Delete EC2-compatible credentials for user per tenant (private network).
`ec2-credentials-get`	Display EC2-compatible credentials.
`ec2-credentials-list`	List EC2-compatible credentials for a user.

Table 16 Unsupported Nova commands

Command	Task
`bare metal-interface-add`	Add a network interface to a bare metal node.
`bare metal-interface-list`	List network interfaces associated with a bare metal node.
`bare metal-interface-remove`	Remove a network interface from a bare metal node.
`bare metal-node-create`	Create a bare metal node.
`bare metal-node-delete`	Delete a bare metal node and any associated interfaces.
`bare metal-node-list`	List available bare metal nodes.
`bare metal-node-show`	Show information about a bare metal node.
`clear-password`	Clear a password for a server.
`cloudpipe-configure`	Update the IP address or port of a cloudpipe instance.
`cloudpipe-create`	Create a cloudpipe instance for a project.
`cloudpipe-list`	List all cloudpipe instances.
`console-log`	Generate console log output for a server. (You cannot use this command for EXS-provisioned instances.)
`coverage-report`	Generate a coverage report.
`coverage-start`	Start Nova coverage reporting.
`coverage-stop`	Stop Nova coverage reporting.
`credentials`	Show user credentials returned from authentication.
`diagnostics`	Retrieve server diagnostics.
`dns-create`	Create a DNS entry for a server domain, name, and IP address.

Table 16 Unsupported Nova commands *(continued)*

Command	Task
`dns-create-private-domain`	Create a private DNS domain.
`dns-create-public-domain`	Create a public DNS domain.
`dns-delete`	Delete a DNS entry.
`dns-delete-domain`	Delete a DNS domain.
`dns-domains`	List available DNS domains.
`dns-list`	List current DNS entries for a domain and an IP address, or for a domain and a server name.
`evacuate`	Evacuate a server from a failed host to a specified host.
`get-password`	Get a password for a server.
`get-spice-console`	Get a SPICE (Simple Protocol for Independent Computing Environments) console for a server.
`host-action`	Perform a power action on a host.
`host-update`	Update host settings.
`interface-attach`	Attach a network interface to an instance.
`interface-detach`	Detach a network interface from an instance.
`interface-list`	List interfaces attached to an instance.
`live-migration`	Migrate a running instance to a new machine.
`lock`	Lock a server.
`migrate`	Migrate a server, enabling the scheduler to select a new host.
`net-create`	Create a network. (You can use this command in Neutron.)
`net-delete`	Delete a network. (You can use this command in Neutron.)
`network-associate-host`	Associate a host with a network.
`network-associate-project`	Associate a project with a network.
`network-create`	Create a network.
`network-disassociate`	Disassociate a host and/or a project from a network.
`pause`	Pause a server. (You cannot use this command for EXS-provisioned instances.)
`rate-limits`	List rate limits for a user.
`rebuild`	Shutdown, re-image, and reboot a server.
`reset-network`	Reset the network of an instance.
`root-password`	Change the root password for a server.
`scrub`	Delete data associated with a project.
`secgroup-add-group-rule`	Add a source group rule to a security group. (You can use this command in Neutron.)
`secgroup-add-rule`	Add a rule to a security group. (You can use this command in Neutron.)
`secgroup-create`	Create a security group. (You can use this command in Neutron.)
`secgroup-delete`	Delete a security group. (You can use this command in Neutron.)

Table 16 Unsupported Nova commands *(continued)*

Command	Task
`secgroup-delete-group-rule`	Delete a source group rule from a security group. (You can use this command in Neutron.)
`secgroup-delete-rule`	Delete a rule from a security group. (You can use this command in Neutron.)
`secgroup-list-rules`	List rules for a security group.
`unpause`	Unpause a server. (You cannot use this command for EXS-provisioned instances.)
`unrescue`	Place a server that is in rescue mode back into active mode.
`x509-create-cert`	Create an x509 certificate for a user in a tenant (private) network.
`x509-get-root-cert`	Get an x509 certificate for a user in a tenant (private) network.

Table 17 Unsupported Glance commands

Command	Task
`add`	Add a new image.
`clear`	Clear an image.
`delete`	Delete an image.
`details`	List details about images you can access.
`image-members`	List information about sharing permissions by image or tenant (private network).
`index`	List an index of images you can access.
`member-add`	Share an image with a tenant (private network).
`member-images`	List information about sharing permissions by image or tenant (private network).
`members-replace`	Replace a shared image.
`show`	Show a description of an image.
`update`	Update an image.

Table 18 Unsupported Cinder commands

Command	Task
`backup-create`	Create a backup.
`backup-delete`	Delete a backup.
`backup-list`	List all backups
`backup-restore`	Restore a backup.
`backup-show`	Show details about a backup.
`create-image-id`	Create a bootable volume from an image.
`encryption-type-create`	Create a new encryption type for a volume type.
`migrate`	Migrate a volume to a new host or to another region or controller.
`service-disable`	Disable the service.
`service-enable`	Enable the service.
`transfer-accept`	Accept a volume transfer.
`transfer-create`	Create a volume transfer.

Table 18 Unsupported Cinder commands *(continued)*

Command	Task
`transfer-delete`	Undo a volume transfer.
`transfer-list`	List all transfers.
`transfer-show`	Show details about a transfer.
`upload-to-image`	Upload a volume to the OpenStack Image Service as an image.

Table 19 Unsupported Neutron commands

Command	Task
`agent-delete`	Delete an agent.
`agent-update`	Update an agent.
`cisco-credential-create`	Create a credential.
`cisco-credential-delete`	Delete a credential.
`cisco-credential-list`	List credentials that belong to a tenant (private network).
`cisco-credential-show`	Show information about a credential.
`cisco-profile-create`	Create a network profile.
`cisco-profile-delete`	Delete a network profile.
`cisco-network-profile-list`	List network profiles for a tenant (private network).
`cisco-network-profile-show`	Show information about a network profile.
`cisco-network-profile-update`	Update information for a profile.
`cisco-policy-profile-list`	List policy profiles for a tenant (private network).
`cisco-policy-profile-show`	Show information about a policy profile.
`cisco-policy-profile-update`	Update information for a policy profile.
`dhcp-agent-list-hosting-net`	List DHCP agents that are hosting a network.
`dhcp-agent-network-add`	Add a network to a DHCP agent.
`dhcp-agent-network-remove`	Remove a network from a DHCP agent.
`firewall-create`	Create a firewall.
`firewall-delete`	Delete a firewall.
`firewall-list`	List firewalls for a tenant (private network).
`firewall-policy-create`	Create a firewall policy.
`firewall-policy-delete`	Delete a firewall policy.
`firewall-policy-insert-rule`	Insert a rule into a firewall policy.
`firewall-policy-list`	List firewall policies that belong to a tenant (private network).
`firewall-policy-remove-rule`	Remove a rule from a firewall policy.
`firewall-policy-show`	Show information about a firewall policy.
`firewall-policy-update`	Update a firewall policy.
`firewall-rule-create`	Create a firewall policy rule.
`firewall-rule-delete`	Delete a firewall policy rule.

Table 19 Unsupported Neutron commands *(continued)*

Command	Task
`firewall-rule-list`	List firewall rules for a tenant (private network).
`firewall-rule-show`	Show information about a firewall rule.
`firewall-rule-update`	Update a firewall rule.
`firewall-show`	Show information about a firewall.
`firewall-update`	Update a firewall.
`ipsec-site-connection-create`	Create an IPsecSiteConnection.
`ipsec-site-connection-delete`	Delete an IPsecSiteConnection.
`ipsec-site-connection-list`	List IPsecSiteConnections that belong to a tenant (private network).
`ipsec-site-connection-show`	Show information about an IPsecSiteConnection.
`ipsec-site-connection-update`	Update an IPsecSiteConnection.
`lb-agent-hosting-pool`	Get a load balancing agent hosting a pool.
`lb-healthmonitor-associate`	Create a mapping between a load balancing health monitor and a pool.
`lb-healthmonitor-create`	Create a load balancing health monitor.
`lb-healthmonitor-delete`	Delete a load balancing health monitor.
`lb-healthmonitor-disassociate`	Remove a mapping between from a load balancing health monitor to a pool.
`lb-healthmonitor-list`	List load balancing health monitors that belong to a tenant (private network).
`lb-healthmonitor-show`	Show information about a load balancing health monitor.
`lb-healthmonitor-update`	Update a load balancing health monitor.
`lb-member-create`	Create a load balancing member.
`lb-member-delete`	Delete a load balancing member.
`lb-member-list`	Lists health balancing members that belong to a tenant (private network).
`lb-member-show`	Show information about a load balancing member.
`lb-member-update`	Update a load balancing member.
`lb-pool-create`	Create a load balancing pool.
`lb-pool-delete`	Delete a load balancing pool.
`lb-pool-list`	List load balancing pools that belong to a tenant (private network).
`lb-pool-list-on-agent`	Lists the pools on a load balancing agent.
`lb-pool-show`	Show information about a load balancing pool.
`lb-pool-stats`	Retrieve statistics for a load balancing pool.
`lb-pool-update`	Update a load balancing pool.
`lb-vip-create`	Create a load balancing Virtual IP (VIP).
`lb-vip-delete`	Delete a load balancing Virtual IP (VIP).
`lb-vip-list`	List load balancing Virtual IPs (VIPs) that belong to a tenant (private network).
`lb-vip-show`	Show information about a load balancing Virtual IP (VIP).
`lb-vip-update`	Update a load balancing Virtual IP (VIP).

Table 19 Unsupported Neutron commands *(continued)*

Command	Task
net-gateway-connect	Add an internal network interface to a router.
net-gateway-create	Create a network gateway.
net-gateway-delete	Delete a network gateway.
net-gateway-disconnect	Remove a network from a network gateway.
net-gateway-list	List network gateways for a tenant (private network).
net-gateway-show	Show information about a network gateway.
net-gateway-update	Update the name of a network gateway.
queue-create	Create a queue.
queue-delete	Delete a queue.
queue-list	List queues that belong to a tenant (private network).
queue-show	Show information about a queue.
service-provider-list	List service providers.
vpn-ikepolicy-create	Create a VPN Internet Key Exchange (IKE) policy.
vpn-ikepolicy-delete	Delete a VPN Internet Key Exchange (IKE) policy.
vpn-ikepolicy-list	List VPN Internet Key Exchange (IKE) policies that belong to a tenant (private network).
vpn-ikepolicy-show	Show information about a VPN Internet Key Exchange (IKE) policy.
vpn-ikepolicy-update	Update a VPN Internet Key Exchange (IKE) policy.
vpn-ipsecpolicy-create	Create a VPN IP security (IPsec) policy.
vpn-ipsecpolicy-delete	Delete a VPN IP security (IPsec) policy.
vpn-ipsecpolicy-list	List VPN IP security (IPsec) policies that belong to a tenant (private network).
vpn-ipsecpolicy-show	Show information about a VPN IP security (IPsec) policy.
vpn-ipsecpolicy-update	Update a VPN IP security (IPsec) policy.
vpn-service-create	Create a VPN service.
vpn-service-delete	Delete a VPN service.
vpn-service-list	List VPN service configurations that belong to a tenant (private network).
vpn-service-show	Show information about a VPN service.
vpn-service-update	Update a VPN service.

E Limitations on support for OpenStack functionality in the CloudSystem Portal

The following table lists OpenStack functions that are not supported or are supported with limitations in the CloudSystem Portal.

Table 20 Limitations on support for OpenStack functionality in the CloudSystem Portal

Function	Task	Limitation
Admin→System Panel→Flavors→More→View Extra Specs	View additional specifications for a flavor.	Not supported
Admin→System Panel→Images→Edit→Update Image→Kernel ID	Specify the ID of an image used as the kernel when booting the image.	Not supported
Admin→System Panel→Images→Edit→Update Image→Ramdisk ID	Specify the ID of an image used as the RAM disk when booting the image.	Not supported
Admin→System Panel→Images→Edit→Update Image→Format	Specify the format of the disk containing an image.	Not supported
Admin→System Panel→Images→Edit→Update Image→Architecture	Specify the operating system architecture of an image.	Not supported
Admin→System Panel→Networks→Create Network→External Network	Create more than one External Network and more than one External Network subnet.	Not supported
Admin→System Panel→Networks→External Network→Edit Network	Edit the External Network and the External Network subnet.	Not supported
Admin→System Panel→System Info→Availability Zones	View information about availability zones configured for host compute nodes.	Not supported
Admin→System Panel→System Info→Host Aggregates	View information about host aggregates configured for compute nodes.	Not supported
Admin→Identity Panel→Projects	Configure an “Administrator” project.	You cannot edit, disable, or delete the “Administrator” project.
Admin→Identity Panel→Users	Configure user information.	You cannot disable, delete, or edit information about a portal user who is an “Infrastructure administrator” user in the CloudSystem Console.
Project→Manage Compute→Instances→Launch Instance→Details→Availability Zone	Select an availability zone for the host compute node of an instance.	Not supported
Project→Manage Compute→Instances→Launch Instance→Details→Instance Boot Source→Boot from volume	Specify that an instance boots from a selected volume.	Not supported
Project→Manage Compute→Instances→Launch Instance→Details→Instance Boot Source→Boot from image (creates a new volume)	Specify that an instance boots from a selected image, and that a new volume is created when the instance launches.	Not supported
Project→Manage Compute→Instances→Launch Instance→Details→Instance Boot Source→Boot from volume snapshot (creates a new volume)	Specify that an instance boots from a selected volume snapshot, and that a new volume is created when the instance launches.	Not supported

Table 20 Limitations on support for OpenStack functionality in the CloudSystem Portal *(continued)*

Function	Task	Limitation
Project→Manage Compute→Instances→Launch Instance→Access & Security→Admin Pass	Specify the administrator password used for accessing an instance after it is launched.	Not supported
Project→Manage Compute→Instances→More→View Log→Log	View a console log for an instance.	Not supported for ESX-provisioned instances
Project→Manage Compute→Instances→More→Pause Instance	Pause an instance.	Not supported for ESX-provisioned instances
Project→Manage Compute→Instances→More→Unpause Instance	Unpause an instance.	Not supported for ESX-provisioned instances
Project→Manage Compute→Instances→More→Rebuild Instance→Rebuild Password	Specify a password used to access a rebuilt instance.	Not supported
Project→Manage Compute→Instances→More→Resize Instance	Resize a disk by assigning a new flavor.	Not supported for ESX-provisioned instances
Project→Manage Compute→Volumes→Attach	Attach a volume to an instance.	For ESX-provisioned instances, the disk is not automatically mounted at the specified path. Instead, the specified path generates a disk unit number.
Project→Manage Compute→Images & Snapshots→More→Create Volume	Create a volume for an image.	Not supported for iSCSI or FC volume types
Project→Manage Compute→Images & Snapshots→More→Delete Snapshot	Delete a snapshot.	You cannot delete a snapshot used to create volumes until you delete the volumes created from the snapshot.
Project→Manage Compute→Access & Security→Security Groups	Create or configure a security group.	You must configure VMware vCloud Networking and Security (VCNS) on ESX-provisioned instances.
Project→Management Network→Networks→More→Add Subnet→Subnet→IP Version→IPv6	Create an IPv6 subnet.	Not supported
Project→Management Network→Networks→More→Add Subnet→Subnet→Gateway	Add the IP address of the router providing access to the subnet.	Not supported